PRIVACY? WHAT PRIVACY?: REFORMING THE STATE SECRETS PRIVILEGE TO PROTECT INDIVIDUAL PRIVACY RIGHTS FROM EXPANSIVE GOVERNMENT SURVEILLANCE

MEGAN PUGH*

INTRODUCTION

The state secrets privilege protects the government from being required to release evidence in a court case based on the assertion that court proceedings could disclose confidential information that would endanger

national security.[1] Developed primarily through common law, without a clear textual basis, the state secrets privilege has broadened over the years, to the point where it has become almost impossible for plaintiffs to litigate issues pertaining to their alleged illegal surveillance by the government.[2]

Even after the enactment of the Foreign Intelligence Surveillance Act ("FISA") in 1978,[3] which provides procedures and protections for plaintiffs in electronic surveillance cases,[4] and despite recognition of FISA's displacement of the state secrets privilege by the Ninth Circuit, plaintiffs are still having their cases dismissed for lack of standing as a result of the state secrets privilege.[5] The crux of the problem is that in order for FISA's procedures to apply to electronic surveillance cases, the plaintiff must establish that he or she is "aggrieved" by proving that he or she was personally surveilled by the government.[6] Yet the government has been able to utilize the state secrets privilege to deny plaintiffs the evidence they need to demonstrate that they are "aggrieved."[7] Without that showing, the protections of FISA do not apply.[8] If the plaintiff cannot show that he or she is "aggrieved," the circuit courts generally default to applying the common law *Reynolds* "reasonable danger" test,[9] which is more arduous for plaintiffs. The application of *Reynolds* results in the dismissal of electronic surveillance cases for lack of standing.[10]

This Note argues that Congress should adopt legislation addressing the state secrets privilege that will provide a statutory basis affording

---

* Juris Doctor Candidate, Belmont University College of Law, 2022; B.S.B.A., Hawai'i Pacific University, 2018. I would like to dedicate this Note to my beloved brother, Harry Pugh, for always encouraging me to think outside of the box. A special thank you to Professor Jeffrey Usman for his continuous guidance and support, and all the editors of *Belmont Law Review* for their diligent work in editing this Note.

1. *See* United States v. Reynolds, 345 U.S. 1, 6–8 (1953).

2. *See generally* Timothy Bazzle, *Shutting the Courthouse Doors: Invoking the State Secrets Privilege to Thwart Judicial Review in the Age of Terror*, 23 GEO. MASON U. CIV. RTS. L.J. 29, 2012.

3. 50 U.S.C. § 1806(f).

4. Joshua T. Lobert, Cong. Rsch. Serv., FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW 1 (2020).

5. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *48–49 (N.D. Cal. Apr. 25, 2019).

6. 50 U.S.C. § 1806(f).

7. *See Jewel*, 2019 U.S. Dist. LEXIS 217140 at *10–11, *46–47.

8. *See id.* at *46–47.

9. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081 (9th Cir. 2010); *see also* Ibrahim v. U.S. Dep't of Homeland Sec., 912 F.3d 1147, 1164 (9th Cir. 2019). *Contra* Sec. and Exch. Comm'n v. Schroeder, No. C07-03798JW, 2008 U.S. Dist. LEXIS 46465 (N.D. Cal. Jan. 15, 2008).

10. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *48–49; *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

plaintiffs a meaningful opportunity to obtain standing and litigate their cases when they have been wrongfully surveilled. In order to mitigate the number of electronic surveillance cases dismissed for lack of standing, this Note suggests a balanced solution that respects national security interests while also providing plaintiffs with a reasonable opportunity to prove standing and litigate their cases.

This Note begins in Section II by exploring the historical evolution of the state secrets privilege. Section III assesses the current impact of the state secrets privilege, noting that it forecloses judicial review of electronic surveillance cases. Section IV describes the current circuit splits over how to apply the state secrets privilege, explaining that this confusion has contributed to judicial deference to the executive branch and dismissal of electronic surveillance cases for lack of standing. Section V examines the government's current approach to surveilling individuals in the United States and why it is important that judicial review be afforded to plaintiffs alleging illegal government surveillance. Section VI addresses constitutional concerns and public policy reasons for why the state secrets privilege needs to be reformed. Section VII proposes a balanced solution, responsive to both privacy and national security interests, that will afford plaintiffs standing in electronic surveillance cases, while still requiring a threshold showing by the plaintiff and appointment of FISA and magistrate judges if necessary. Explaining the reasoning behind the proposed solution, Section VIII argues why Congress should enact such legislation.

I. HISTORY OF THE STATE SECRETS PRIVILEGE

The history of the state secrets privilege has largely contributed to dismissal of electronic surveillance cases for lack of standing due to continuing judicial deference to the executive branch.[11] Beyond Article I, Section 5, Clause 3 of the Constitution, which provides that government secrecy of its proceedings may be required in some situations,[12] the state secrets privilege has developed solely through case law.[13] The state secrets privilege has been broadly interpreted and applied by the circuit courts.[14] The two leading United States Supreme Court cases that have shaped the

11. *See generally Jewel*, 2019 U.S. Dist. LEXIS 217140 at *41–47 (applying the common law created *Reynolds* "reasonable danger" test instead of FISA procedures in dismissing the case on state secrets privilege grounds).

12. Article I, Section 5, Clause 3 of the Constitution states that "Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy." U.S. CONST. art. I, § l5, cl .3.

13. *See generally* Bazzle, *supra* note 2, at 32–54.

14. *See generally* Susan N. Herman, *Ab(ju)dication: How Procedure Defeats Civil Liberties in the "War on Terror"*, 50 SUFFOLK U. L. REV. 79, 93–95 (2017).

state secrets privilege are *Totten v. United States*[15] and *United States v. Reynolds*.[16] *Totten* laid the foundation for the state secrets privilege, requiring courts to dismiss a case if it could lead to the disclosure of matters considered confidential by "the law itself".[17] *Reynolds* expanded the privilege to protect the government from producing certain evidence during litigation that could lead to disclosure of government secrets.[18] *Reynolds* remains the controlling precedent for the state secrets privilege, requiring that courts be deferential to the executive branch as to when disclosure of certain evidence poses a "reasonable danger" to national security.[19]

In the wake of *Totten* and *Reynolds*, the state secrets privilege was often successfully invoked by the government.[20] Yet simultaneously, it became increasingly clear that the government was abusing electronic surveillance.[21] Congress responded by enacting the Foreign Intelligence Surveillance Act ("FISA") in 1978, designed to protect the public from government surveillance abuses and establish procedures for judicial review of surveillance cases.[22] FISA is not all-encompassing for addressing claims of improper governmental surveillance; rather, when surveillance cases do not fall within FISA's purview,[23] the circuit courts return to applying *Reynolds*' "reasonable danger" test, which often results in dismissal of the case altogether.[24]

---

15. Totten v. United States, 92 U.S. 105, 106–07 (1876).

16. United States v. Reynolds, 345 U.S. 1, 7 (1953).

17. *Totten*, 92 U.S. at 107.

18. *Reynolds*, 345 U.S. at 10.

19. *Id.*

20. *See* Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1254 (9th Cir. 2019); *see also* Jewel v. NSA, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *10–12. (N.D. Cal. Apr. 25, 2019).

21. *See generally* James Bovard, *Inspector General report on FBI's FISA abuse tells us one thing: We need radical reform*, USA TODAY (Dec. 10, 2019, 1:38 PM), https://www.usatoday.com/story/opinion/2019/12/10/ig-report-fbi-fisa-abuse-secret-court-trump-campaign-column/4383722002/ [https://perma.cc/7M3U-A7QY]; Jordan Davidson, *FISA Court Confirms The Government Lied In Every Spy Warrant Application Against Carter Page*, THE FEDERALIST (Sept. 17, 2020), https://thefederalist.com/2020/09/17/fisa-court-confirms-the-government-lied-in-every-spy-warrant-application-against-carter-page/ [https://perma.cc/T6XN-MXEM].

22. *See* ELIZABETH B. BAZAN, CONG. RSCH. SERV., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF SELECTED ISSUES 1 (2008).

23. *See* Ibrahim v. U.S. Dep't of Homeland Sec., 912 F.3d 1147, 1164 (9th Cir. 2019); Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1092 n.15 (9th Cir. 2010). *Contra* Sec. and Exch. Comm'n v. Schroeder, No. C07-03798JW, 2008 U.S. Dist. LEXIS 46465 (N.D. Cal. 2008).

24. *See Jewel*, 2019 U.S. Dist. LEXIS 217140 at *48–49; *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

In 1803, the state secrets privilege appeared in primordial form in *Marbury v. Madison* when Marbury demanded that the Secretary of State testify regarding the whereabouts of his commission.[25] The Supreme Court indicated that the Secretary of State "would not have been obliged to impart information communicated to him in confidence."[26] Just a few years later in *United States v. Burr*, the Supreme Court noted that the president does not have to disclose a document at trial that could endanger public safety.[27]

Although it was evident, pursuant to *Marbury* and *Burr*, that a member of the executive branch does not have a duty to disclose information requested by a plaintiff when it was communicated to him or her in confidence, or when its disclosure could endanger public safety, the state secrets privilege was not clearly established by the Supreme Court until *Totten* was decided in 1875.[28] In *Totten*, the plaintiff was the administrator of William Lloyd's estate, seeking to recover compensation owed by the president to Lloyd for services he provided for the government as a secret agent.[29] The Court outright dismissed the case based on separation of powers principles.[30] Specifically, the Court explained that the compensation contract was for *secret* service.[31] Thus, if such a case could be litigated by the judicial branch, details of dealings with individuals might be exposed, and this would be "to the serious detriment of the public."[32] The Court further stated that government secret agents must look to their respective department for their compensation because the court has no business in enforcing secret government contracts.[33] A court action would be available to the public in public records, thus would "itself be a breach of contract of [secret service], and thus defeat recovery."[34]

Overall, *Totten* precluded judicial review of cases that would "inevitably lead to the disclosure of matters which the law itself regards as confidential."[35] *Totten* implied that the state secrets privilege is rooted in separation of powers principles of the constitution and is an absolute bar to litigation if the decision of the case depends on the disclosure of government secrets.[36] *Totten* is rather vague and leaves much open to interpretation.[37] For example, Justice Field very broadly defined what could

25. Marbury v. Madison, 5. U.S. 137, 143–44 (1803).
26. *Id.* at 144–45.
27. United States v. Burr, 25 F. Cas. 30, 37 (C.C.D. Va. 1807).
28. *See generally* Bazzle, *supra* note 2, at 33–35.
29. Totten v. United States, 92 U.S. 105, 105–06 (1876).
30. *Id.* at 106.
31. *Id.* (emphasis added).
32. *Id.* at 106–07.
33. *Id.* at 107.
34. *Id.*
35. *Id.*
36. *See generally* Bazzle, *supra* note 2, at 34–35.
37. *Id.*

be covered by the state secrets privilege, noting that "all secret employments of the government in time of war, or upon matters affecting our foreign relations, where a disclosure of the service *might compromise or embarrass* [the] government in its public duties, or endanger the person or *injure the character of the agent*" should not be litigated by the judicial branch.[38] Justice Field indicates that to prevent a plaintiff from litigating a government surveillance case, the government need only show that the case could cause potential embarrassment or mere injury to the character of a government agent.[39]

Additionally, Justice Field wrote that "public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which *the law itself regards as confidential*."[40] This gives a judge very broad discretion to determine what the law deems confidential with regard to national security. Justice Field noted that confidences of the confessional, confidences between husband and wife, attorney-client privilege, and doctor-patient privilege are some corollaries,[41] but without additional guidance, the statement is so vague that it is challenging for a plaintiff to truly know whether his or her case could involve a matter that the law regards as confidential.[42] Providing such examples is also problematic because it indicates that cases merely *involving* any regular privilege as suggested in the Federal Rules of Evidence could preclude litigation of the case completely.[43] Essentially, Justice Field's statements in *Totten* created the state secrets privilege, making it a total bar to litigation wherein the judicial branch could not review cases which would "inevitably lead to disclosure of matters that the law regards as confidential."[44] Without a clear standard for what the law regards as confidential, or more guidance as to what Justice Fields meant by such a statement, *Totten* left the state secrets privilege open to broad interpretation.[45]

In 1953, *Reynolds*[46] expanded the application of the state secrets privilege, indicating that it can be also be invoked as a means to protect the government from being required to produce certain *evidence* during litigation that could *lead to* disclosure of government secrets.[47] In *Reynolds*, the plaintiffs sued the government for a military plane crash that caused the

38. *Totten*, 92 U.S. at 106.
39. *See generally id.* at 106–07.
40. *Id*. at 107.
41. *Id.*
42. *See generally* Bazzle, *supra* note 2, at 34–35.
43. *See generally id.*
44. *Id.* at 34 (quoting *Totten,* 92 U.S. at 105–06).
45. *See generally id.* at 34–35.
46. United States v. Reynolds, 345 U.S. 1 (1953).
47. *Id.* at 10.

deaths of their spouses.[48] The plaintiffs moved for production of the Air Force's official accident investigation report and statements of the surviving crew members that were taken in connection with the official investigation.[49] The government claimed that the evidence was privileged, and the court agreed that the government did not need to produce such information since there was a "reasonable danger" that compulsion of the evidence would expose military matters that "should not be divulged."[50] The Court explained that the only reason the military plane took flight was to test secret electronic equipment, so there was certainly a reasonable danger that the accident investigation report would contain references to secret electronic equipment that was the entire reason for undergoing the mission to begin with.[51]

In reaching its ultimate conclusion, the Court focused on a showing of necessity, stating that when a plaintiff demonstrates a strong necessity for production of the evidence, "the claim of privilege should not be lightly accepted," but also noting that even the most compelling necessity cannot overcome the privilege when military secrets are at stake.[52] The Court explained that the plaintiffs were offered the opportunity to examine the surviving crew members themselves, but did not do so, which shows a weak necessity for the privileged evidence.[53] By examining the survivors themselves, the plaintiffs should have been able to adduce essential facts indicating the cause of the plane crash without requiring disclosure of evidence that could expose military secrets.[54]

Reynolds shaped the modern understanding of the state secrets privilege, indicating that courts must be deferential to the executive branch as to when disclosure of evidence would pose a "reasonable danger" to national security.[55] The Court suggested that judges can base the degree of deference to the executive branch in part upon the importance of the contested information to the plaintiff's case: the greater the plaintiff's need for the evidence, the more scrutiny courts should exercise when the government invokes the privilege.[56] If the plaintiff can instead rely on alternative, non-privileged information to support his or her claim, the court may give more deference to the government.[57]

After *Totten* and *Reynolds*, the state secrets privilege has been frequently claimed by the government in surveillance cases to avoid

48. *Id.* at 3.
49. *Id.*
50. *Id.* at 10.
51. *Id.*
52. *Id.* at 10.
53. *Id.* at 11.
54. *Id.*
55. *Id.* at 10.
56. *Id.* at 11.
57. *Id.*

production of documents in discovery or evade litigation altogether.[58] With no statutory basis, the claim of privilege was generally successful when invoked by the government.[59] As it became increasingly clear that the government was abusing electronic surveillance for national security purposes, Congress responded.[60] Congress enacted FISA in 1978 as an attempt to lessen electronic surveillance abuse and create clearer procedures for handling surveillance cases.[61] The purpose of FISA is to provide judicial and congressional oversight of electronic surveillance activities while maintaining secrecy that is necessary to monitor national security threats.[62]

However, following 9/11, the government expanded its surveillance powers to protect the United States from terrorism, incidentally weakening FISA's protections.[63] Congress first passed the US Patriot Act (2001), which strengthened government surveillance and removed numerous obstacles to investigating terrorism.[64] The executive branch also engaged in three key programs to expand government surveillance: Project Stellarwind, PRISM, and Upstream.[65] Project Stellarwind allowed the National Security Agency ("NSA") to monitor call and text metadata of United States citizens and tap any international calls that included a United States-based caller.[66] PRISM is an NSA internet surveillance tool created to collect the private internet data of foreign nationals. However, in doing so, it also sweeps up the data of United States citizens, including emails, files and photos, through accessing user accounts on Gmail, Facebook, Apple, Microsoft and other technology companies.[67] Upstream infiltrates the infrastructure of the Internet to copy and filter traffic from PRISM.[68] Furthermore, FISA itself has also been repeatedly amended to address changing circumstances.[69] For

58. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *10–11. (N.D. Cal. Apr. 25, 2019).

59. *See Jewel*, 2019 U.S. Dist. LEXIS 217140 at *48–49; *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

60. For a study revealing abuses of electronic surveillance for national security purposes and uncertainty surrounding state law on the subject, see BAZAN, *supra* note 22, at 1.

61. *See id.*

62. U.S. DEP'T OF JUST., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (2013).

63. *See* Anna Dorothea Ker, *United States of Surveillance*, THE PRIVACY ISSUE, Jan. 22, 2020, https://theprivacyissue.com/government-surveillance/united-states-of-surveillance-us-history-spying [https://perma.cc/C7WT-5E58].

64. *See* Richard Horowitz, *Summary of Key Sections of the USA Patriot Act of 2001*, 1–3, patriot_act_summary.pdf (rhesq.com) [https://perma.cc/8DFZ-C8HW] (last visited Aug. 1, 2021).

65. *See* Ker, *supra* note 63.

66. *See id.*

67. *See id.*

68. *See id.*

69. BAZAN, *supra* note 22, at 2.

example, the FISA Amendments Act of 2008 broadened government surveillance powers through relaxing warrant requirements for surveillance and adding Section 702, which is addressed in greater detail below.[70]

As originally enacted in 1978, FISA created a statutory framework for collection of foreign intelligence information through the use of electronic surveillance.[71] It established the Foreign Intelligence Surveillance Court (FISC) to hold nonpublic sessions to consider issuing search warrants under FISA, and required most electronic surveillance to be authorized by a court order, obtained by submitting a detailed application with specific requirements to FISC.[72] The 1978 version of FISA further permitted the Attorney General to authorize emergency employment of electronic surveillance if the appropriate judge is informed of the authorization and the Attorney General submits an application to that judge within 24 hours of authorization.[73] However, the government is prohibited from using any information concerning a United States person acquired from disapproved emergency surveillance without their consent.[74]

In 2008 Congress adopted the FISA Amendments Act to broaden government surveillance powers under FISA in an attempt to strengthen national security.[75] The Act removed the requirement for intelligence agencies to obtain a warrant in order to surveil communications between United States persons and foreign targets.[76] The Act also added Section 702, allowing the government to compel assistance of electronic communications service providers for up to one year in targeting non-United States persons reasonably believed to be located outside the United States.[77] The FISC may now approve surveillance without requiring individualized applications for each target, so long as the government "reasonably believes" the targets are located outside the United States.[78] Section 702 thus authorizes collection, use, and dissemination of electronic communications content stored by U.S. internet service providers such as Google, Facebook, and Microsoft, and compels assistance of U.S. telecommunications providers such as AT&T and Verizon.[79] Yet Section 702 does not *require* the surveillance target be a suspected terrorist, spy, or

70. Lobert, *supra* note 4, at 2.
71. *Id.* at 1.
72. S. 1566, 95th Cong. (1977) (enacted).
73. *See id.*
74. *See id.*
75. *See generally* H.R. 6304, 110th Cong. (2008) (enacted).
76. *See id.*
77. *See id.*
78. *See id.*
79. Greg Nojeim, *Section 702: What It Is & How It Works*, CTR. FOR DEMOCRACY AND TECH. (Feb. 15, 2017), https://cdt.org/insights/section-702-what-it-is-how-it-works/ [https://perma.cc/KH84-8KXN].

agent of a foreign power.[80] On the contrary, Section 702 requires that targets be non-United States persons located abroad, and that a *significant purpose* behind the surveillance is to obtain foreign intelligence information.[81] With such broad language and flexible requirements, Section 702 has led to surveillance abuses and has been the subject of much controversy, brought to light in 2013 when Edward Snowden leaked documents indicating that Section 702 has resulted in the incidental collection of communication between thousands of innocent Americans.[82]

II. CONTEMPORARY FUNCTIONING OF THE STATE SECRETS PRIVILEGE

In order to understand the problems with the state secrets privilege as it functions today, it is important to consider how current legislation and case law interact with the state secrets privilege. First, use of electronic information under FISA has been codified in 50 U.S.C. § 1806, establishing procedures for use of confidential evidence in cases alleging wrongful surveillance.[83] However, these procedures only apply to cases of electronic surveillance when the plaintiff establishes that he or she is "aggrieved" under FISA.[84] Second, since its 2008 amendments, FISA was again amended in 2018 to extend government foreign intelligence collection powers.[85] This extension of powers has moved FISA further away from its original goal of narrowing government surveillance abuses, instead creating an avenue for more potential surveillance abuses.[86] Third, *Reynolds* has broadened the state secrets privilege, allowing the government to invoke it at an early stage of litigation and serving as the default test for electronic surveillance cases when FISA does not apply,[87] thus leading to frequent dismissal of electronic surveillance cases for lack of standing.[88] Fourth, recent case law demonstrates that FISA only seems to protect against the state secrets privilege for plaintiffs who already have, prior to discovery,

---

80. *Id.*

81. *Id.*

82. *See FISA: 702 Collection*, LAWFARE INST., https://www.lawfareblog.com/topic/fisa-702-collection [https://perma.cc/T38C-WAA6] (last visited Aug. 1, 2021).

83. *See* 50 U.S.C. § 1806(f) (2021).

84. *See id.*

85. *See generally* S. 139, 115th Cong. (2018) (enacted).

86. *See generally* Charlie Savage et al., *House Extends Surveillance Law, Rejecting New Privacy Safeguards*, N.Y. TIMES (Jan. 11, 2018), https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html [https://perma.cc/4CQ3-2CZG].

87. *See* Jewel v. Nat'l Sec. Agency, No. C 08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *41 (N.D. Cal. Apr. 25, 2019).

88. *See id.* at *48–49; *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

the evidence needed to prove their *prima facie* case.[89] Specifically, in *Fazaga v. FBI*, the plaintiffs defeated the government's state secrets privilege claim but already had the evidence needed for their *prima facie* case prior to trial.[90] Yet just months later, *Jewel v. NSA* was dismissed for lack of standing, with the evidence needed to prove standing still in the hands of the government, protected by a state secrets privilege claim.[91] Finally, Congress recently attempted to limit surveillance powers under FISA by introducing the Safeguarding Americans Private Records Act (2020),[92] the USA Freedom Reauthorization Act (2020),[93] and the Protecting Our Civil Liberties Act (2020).[94] However, none of these Acts address litigation of surveillance cases against the government nor make any attempt to reform the judicial process for plaintiffs to achieve standing in such cases.[95]

FISA's limited application to only surveillance cases in which the plaintiff qualifies as "aggrieved," combined with new FISA amendments that have increased potential for government surveillance abuses, have created significant problems with contemporary application of the state secrets privilege.[96] Current case law demonstrates that courts will default to applying the common law state secrets privilege "reasonable danger" test from *Reynolds* when the plaintiff does not qualify as "aggrieved" under FISA.[97] As a result, plaintiffs are having their cases dismissed for lack of standing with no opportunity to seek redress for potentially illegal government surveillance.[98] Congress's recent legislation attempts do not address this standing problem,[99] which means that new legislation needs to be enacted.

---

89. *See, e.g.*, Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1248 (9th Cir. 2019).

90. *See id.*

91. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *37.

92. Safeguarding Americans' Private Records Act of 2020, S. 3242, 116th Cong. (2019-2020).

93. USA Freedom Reauthorization Act of 2020, H.R. 6172, 116th Cong. (2019-2020).

94. Protect Our Civil Liberties Act, H.R. 8970, 116th Cong. (2019-2020).

95 *See* S. 3242, 116th Cong. (2019-2020); H.R. 6172, 116th Cong. (2019-2020); H.R. 8970, 116th Cong. (2019-2020).

96. *See Jewel*, 2019 U.S. Dist. LEXIS 217140 at *48–49; *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

97. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081 (9th Cir. 2010); *see also* Ibrahim v. U.S. Dep't of Homeland Sec., 912 F.3d 1147, 1164 (9th Cir. 2019). *Contra Sec. and Exch. Comm'n* v. Schroeder, No. C07-03798JW, 2008 U.S. Dist. LEXIS 46465 (N.D. Cal. Jan. 15, 2008).

98. *See Jewel*, 2019 U.S. Dist. LEXIS 217140 at *48–49; *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

99. *See* S. 3242, 116th Cong. (2019-2020); H.R. 6172, 116th Cong. (2019-2020); H.R. 8970, 116th Cong. (2019-2020).

A. 50 U.S.C. § 1806 Procedures for Use of Information

FISA's procedures for government electronic surveillance have been codified in 50 U.S.C. § 1806.[100] 50 U.S.C.§ 1806(f) requires that whenever an "aggrieved" plaintiff requests materials from the government related to or derived from electronic surveillance, and the Attorney General files an affidavit that disclosure would harm the national security of the United States, the court must review materials relating to the surveillance *in camera* and *ex parte*.[101] In conducting this review, the court must review all that is necessary to determine whether the surveillance of the aggrieved plaintiff was lawfully authorized and conducted.[102] In civil and criminal cases, the court may disclose to the plaintiff materials related to the surveillance that are necessary to make an accurate decision about the legality of the surveillance.[103] In criminal cases, if the court determines that the surveillance was not lawfully authorized and conducted, it should suppress the unlawfully obtained evidence.[104] Even if the surveillance is found to have been lawfully authorized or conducted in a criminal case, the court may still allow disclosure or require discovery *to the extent that due process requires*.[105]

However, 50 U.S.C. § 1806 procedures only apply to "aggrieved" persons.[106] For plaintiffs to prove they are "aggrieved" within the meaning of FISA, they must show that they themselves were the target of electronic surveillance or had their communications or activities surveilled.[107] As in any case, plaintiffs also still need to establish Article III standing to have their case heard.[108] Similar to FISA's requirement that the plaintiff be "aggrieved," standing requires that the plaintiff show a concrete and particularized injury that is actual or imminent.[109] Standing also requires proof of causation between the injury and the conduct complained of,[110] and it must be likely that the injury will have a remedy by a court's favorable decision.[111]

---

100. *See* 50 U.S.C. § 1806(f).
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.* § 1806(g).
105. *Id.*
106. *Id.* § 1806(f).
107. *Id.* § 1801(k).
108. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992); *see also* Allen v. Wright, 468 U.S. 737, 752 (1984); Warth v. Seldin, 422 U.S. 490, 498–99 (1975).
109. *See Lujan,* 504 U.S. at 555.
110. *See* Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 61–62 (1976).
111. *See Allen,* 468 U.S. at 752.

B. FISA Amendments Reauthorization Act (2018)

The FISA Amendments Reauthorization Act of 2017 reauthorized Title VII of FISA until December 31, 2023, and amended it to further enhance government foreign intelligence collection powers.[112] The Act extended the FISA Amendments Act of 2008 (thereby extending Section 702 authority), made minimal changes to the National Security Agency ("NSA") program, and added an "emergency authorization" provision, which eliminated oversight of subsequent orders to surveil United States citizens.[113] Specifically, the "emergency authorization" provision allows the Attorney General, after initially authorizing emergency employment of electronic surveillance, to subsequently order (without permission) the targeting of a *United States* person subject to emergency employment of electronic surveillance who is *reasonably believed* to be located outside the United States.[114] This means that once already authorized to conduct a search of a non-United States person due to an emergency situation, the Attorney General may then surveil United States persons without a court order.[115]

Surveillance procedures have raised some concerns over the past few years pursuant to the release of declassified opinions from the FISC.[116] These opinions indicate that under Section 702 of FISA, the NSA acquired additional communications between untargeted persons if the communications were "about" the targeted identifier.[117] Americans were essentially surveilled even if they were not targets of surveillance.[118] Although the NSA announced in 2017 that it ceased acquiring additional communications "about" the targeted identifier,[119] controversy still remains

112. *See* Statement on Signing the FISA Amendments Reauthorization Act of 2017, 2018 DAILY COMP. PRES. DOC. 201800040 (Jan. 19, 2018).

113. *See generally* FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018).

114. *Id.*

115. *See* Chinmayi Sharma, *Summary: FISA Amendments Reauthorization Act*, LAWFARE (Oct. 27, 2017, 3:30 PM), https://www.lawfareblog.com/summary-fisa-amendments-reauthorization-act [https://perma.cc/VGF4-3KKJ].

116. EDWARD C. LIU, CONG. RSCH. SERV., SUMMARY OF THE SUBSTANTIVE PROVISIONS OF S. 2010, THE FISA AMENDMENTS REAUTHORIZATION ACT OF 2017, AND H.R. 3989, THE USA LIBERTY ACT OF 2017, at 5 (2017).

117. *Id.* at 5–6.

118. *See generally id.*

119. *Id.* at 6.

over NSA's superfluous surveillance of individuals and whether the NSA is still abusing electronic surveillance.[120]

C. Aftermath of *Reynolds*

In addition to FISA's limited application to only "aggrieved" plaintiffs and FISA amendments that have weakened surveillance protections, there are two key consequences of the Supreme Court's decision in *Reynolds* that have largely contributed to the current problem with the state secrets privilege. First, circuit courts have interpreted *Reynolds* as meaning that if the court finds the "very subject matter" of a case to be a state secret, it should be dismissed outright.[121] Yet *Reynolds* allows the state secrets privilege to be invoked at an early stage of litigation, so the circumstances that the judge must analyze are limited to what has been plead and what the government has submitted in the form of affidavits.[122] At such an early stage, judges must often determine whether evidence should be removed from trial by looking not at the evidence itself, but at what one party says the evidence is.[123] Therefore, judges must determine whether the "very subject matter" of the case is a state secret, and consequently dismiss the case, without having a complete record of the evidence.

---

120. *See* ACLU, *NSA Surveillance*, https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance [https://perma.cc/WT62-G3DP] (last visited Aug. 1, 2021) (stating that the FISA Amendment Acts of 2008 gave the NSA unchecked power to monitor Americans' international phone calls, text messages, and emails); *see also* Martin Matishak, *Powerful Lawmakers Join Effort to Kill Surveillance Program Protected by Trump Administration*, POLITICO (Jan. 25, 2020), https://www.politico.com/news/2020/01/25/nsa-surveillance-program-congress-104023 [https://perma.cc/BED2-EK6A] (explaining that Senate and House members are still pushing to end NSA's surveillance program that gathers records of Americans' telephone calls and text messages in search of potential terrorist connections).

121. *See, e.g.*, Kasza v. Browner, 133 F.3d 1159, 1166–67 (9th Cir. 1998). This confusion was created because *Reynolds* stated that "where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake" and then supported this assertion with "*see* Totten v. United States, 92 U.S. 105 (1875), where the very subject matter of the action, a contract to perform espionage, was a matter of state secret. The action was dismissed on the pleadings without ever reaching the question of evidence, since it was so obvious that the action should never prevail over the privilege". United States v. Reynolds, 345 U.S. 1, 11 n.26 (1953).

122. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW**,** 2019 U.S. Dist. LEXIS 217140, at *48–49 (Cal. D. Ct. Apr. 25, 2019).

123. *See generally Jewel***,** 2019 U.S. Dist. LEXIS 217140, at *23–24.

The second key issue with *Reynolds* is that its "reasonable danger" test is still applied by courts today in electronic surveillance cases when FISA procedures do not apply,[124] yet it is an outdated decision that does not account for the surveillance advancements that have occurred since the decision.[125] As explained in Section II, the "reasonable danger" test requires that courts defer to the executive branch as to when disclosure of allegedly privileged evidence would pose a "reasonable danger" to national security, essentially requiring dismissal of the case without the court reviewing the allegedly privileged evidence.[126] Since 1953, technological advancements and surveillance capabilities have excelled.[127] When the Supreme Court wrote the *Reynolds* opinion in 1953, the government was not surveilling individuals like it is today because the technology to do so did not yet exist.[128] As Section V will explain, current government surveillance places individual rights at risk,[129] so it is concerning that electronic surveillance cases are being dismissed based on a test developed in 1953 without first requiring judicial review of the allegedly privileged evidence. Furthermore, *Reynolds* is clearly outdated because it directly conflicts with FISA, enacted 25 years later and requiring *ex parte* and *in camera* review of allegedly privileged materials by the judge when the plaintiff is "aggrieved."[130] In contrast to FISA, *Reynolds* implied that judges should not review allegedly privileged material at all, stating that even an examination of the evidence by the judge alone in his or her chambers would "jeopardize the security which the [state secrets] privilege is meant to protect."[131]

---

124. *See id.* at *41, *43.

125. *See generally Reynolds*, 345 U.S. at 1–12 (this case was decided in 1953); April White, *A Brief History of Surveillance in America*, SMITHSONIAN MAG. (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ [https://perma.cc/HZ5F-UTXF] (indicating that contemporaneously, electronic surveillance operates on a mass scale, whereas electronic surveillance was highly individualized up until the 1980s).

126. *Reynolds*, 345 U.S. at 10.

127. *See generally* James Byrne & Gary Marx, *Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact*, 20 CAHIERS POLITIESTUDIES 17–40 (2011).

128. *See generally* White, *supra* note 125.

129. *See* ACLU, *Privacy and Surveillance*, https://www.aclu.org/issues/national-security/privacy-and-surveillance [https://perma.cc/SF82-AZ9M] (last visited Aug. 1, 2021).

130. *See* 50 U.S.C. § 1806(f).

131. *Reynolds*, 345 U.S. at 10.

D. Fazaga v. Federal Bureau of Investigation (2019)

FISA's protections were put to the test in 2019. [132] In *Fazaga*, the plaintiffs sued the FBI pursuant to another case that revealed they were potentially surveilled by the FBI.[133] Between 2006 and 2007, the FBI paid an informant named Monteilh to gather information as part of Operation Flex.[134] Monteilh recorded numerous conversations with Muslims in the area where the plaintiffs resided, including at mosques which the plaintiffs attended.[135] Having interacted with Monteilh, and following subsequent confirmation from the FBI and Monteilh himself that Monteilh worked for the FBI, the plaintiffs filed suit alleging numerous constitutional violations.[136] Although the FBI had already publicly disclosed that Monteilh created audio and video recordings, and sent handwritten notes to the FBI, the FBI nevertheless claimed state secrets privilege on certain information concerning Operation Flex and Monteilh's activities.[137]

In assessing the plaintiff's electronic surveillance claims, the court determined that by enacting FISA, Congress displaced the common law dismissal remedy created by *Reynolds* in cases of electronic surveillance that fall within FISA's purview.[138] Specifically, FISA procedures are to be used when an "aggrieved" person, someone who can prove they were personally electronically surveilled, affirmatively challenges the legality of electronic surveillance or its use in litigation.[139] The court explained that the state secrets privilege is an evidentiary rule, not constitutional law, and that Congress intended to make FISA's 50 U.S.C. § 1806(f) *in camera* and *ex parte* procedure the *exclusive* procedure for evaluating evidence that threatens national security in the context of electronic surveillance-related determinations.[140] Since the plaintiffs in *Fazaga* already had clear evidence that Monteilh was an informant and surveilled Muslims for the FBI, and that they had interacted with him on numerous occasions, the plaintiffs had adequate evidence to show that they were "aggrieved."[141] The court consequently allowed a number of the plaintiffs' claims to go forward, thus defeating some of the government's state secrets privilege claims.[142]

---

132. *See generally* Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1231 (9th Cir. 2019).
133. *See id.* at 1214.
134. *Id.* at 1212.
135. *Id.*
136. *Id.* at 1214.
137. *Id.* at 1215.
138. *Id.* at 1231.
139. *Id.* at 1238.
140. *Id.* at 1231.
141. *Id.* at 1254.
142. *Id.*

In *Fazaga*, the Ninth Circuit became the first federal Circuit Court to hold that FISA's procedures displace the state secrets privilege in cases of electronic surveillance when the plaintiff qualifies as "aggrieved."[143] This displacement alters the standard of review by which judges assess surveillance cases for plaintiffs who qualify under FISA. Under the *Reynolds* common law state secrets privilege, the court must evaluate whether requiring evidence over which the state secrets privilege has been asserted would pose a "reasonable danger" to national security.[144] If it would pose a reasonable danger, the evidence need not be disclosed even if it includes evidence of government wrongdoing.[145] Alternatively, for parties falling under FISA's procedures, the court determines if the surveillance of an aggrieved person was lawfully authorized and conducted.[146] The court may then disclose to the plaintiff materials related to the surveillance that are necessary to make an accurate decision about the legality of the surveillance,[147]and suppress the evidence in a criminal case if it was not lawfully authorized and conducted.[148] Even if the surveillance is found to have been lawfully authorized or conducted in a criminal case, the court may still allow disclosure or discovery if necessary for due process.[149] FISA thus places a different inquiry on issues of electronic surveillance, emphasizing the plaintiff's interests more than the government's by requiring judges to determine if the surveillance was lawfully authorized or conducted instead of just determining whether disclosure of the evidence would pose a reasonable danger to national security.[150]

E. Jewel v. National Security Agency (2019)

Pursuant to *Fazaga*, it appeared that, by using FISA procedures, courts would provide an avenue for recourse for improper government surveillance instead of dismissing the case based on *Reynolds*.[151] However,

---

143. *Id.* at 1225.

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

145. El-Masri v. United States, 479 F.3d 296, 305–06 (4th Cir. 2007).

146. 50 U.S.C. § 1806(f).

147. *Id.*

148. *Id.* § 1806(g).

149. *Id.*

150. *Cf.* United States v. Reynolds, 345 U.S. at 10 (1953). *See generally id.* § 1806(f).

151. *See generally* ACLU OF S. CAL, *Landmark Legal Ruling Permits Courts to Review Claims of Unlawful Surveillance of Muslims*, (Feb. 28, 2019), https://www.aclusocal.org/en/press-releases/landmark-legal-ruling-permits-courts-review-claims-unlawful-surveillance-muslims [https://perma.cc/GSW3-2Y9Q]; Cindy A. Cohn, *9th Circuit can restore balance in national security cases*, DAILY J. (Jan. 27, 2020), https://www.dailyjournal.com/articles/356021-9th-circuit-can-restore-balance-in-national-security-cases [https://perma.cc/F59W-TRU8].

this is not what occurred.[152] *Fazaga*'s significance was undermined just a few months later when the Ninth Circuit faced yet another case of alleged wrongful surveillance.[153] In *Jewel v. NSA*, the court held that "the very issue of standing implicates state secrets," and dismissed the case on state secrets grounds.[154] FISA did not protect the plaintiffs from the government's state secrets privilege claim, because the evidence that the plaintiffs needed to prove that they were "aggrieved" under FISA was itself subject to invocation of the state secrets privilege.[155] Thus, instead of applying FISA procedures to the case, the court applied the common law *Reynolds* state secrets privilege.[156]

In *Jewel*, the plaintiffs filed a class action against the government for conducting warrantless dragnet surveillance of United States citizens with the assistance of telecommunications companies, without a warrant or court order.[157] The court noted that to have standing, the plaintiffs needed to show they suffered an injury in fact, fairly traceable to the defendants, that could be redressed by the courts.[158] The plaintiffs needed to show that their metadata was collected by the government.[159] However, the government claimed state secrets privilege on evidence that the plaintiffs needed to show that their metadata was collected by the government.[160] To prove that they had standing, the plaintiffs had declarations of former AT&T technicians and a former AT&T employee,[161] a FISC order authorizing the NSA to collect bulk data for 90 days, a letter from an NSA Inspector General regarding a non-compliance incident in the telephone call records program, and a working draft of a report prepared by the Office of the NSA Inspector General.[162] Nevertheless, barred from discovery, the plaintiffs could not adequately prove that their own metadata was collected by the government, so the court held their evidence insufficient to demonstrate standing.[163]

The court conducted an *ex parte* and *in camera* review of what limited classified materials were available at such an early stage of litigation as required by FISA's § 1806 procedures,[164] but never decided

152. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140 at *48–49 (N.D. Cal. Apr. 25, 2019).
153. *See id.* at *7–52.
154. *Id.* at *48–49.
155. *Id.* at *11.
156. *Id.* at *16–17.
157. *Id.* at *7–8.
158. *Id.* at *19.
159. *Id.* at *19–20.
160. *Id.* at *11.
161. *Id.* at *28–31.
162. *Id.* at *33–35.
163. *Id.* at *36.
164. *See* 50 U.S.C. § 1806(f).

the question of whether government surveillance of the plaintiffs was lawfully authorized and conducted,[165] as FISA also requires.[166] The court ultimately decided that, even if there were sufficient evidence that the plaintiffs' metadata was collected by the government, a finding of standing would necessitate disclosure of possible interceptions of the plaintiffs' communications, a disclosure which in itself "may imperil national security."[167] The court stated that proceeding further with the case would "cause exceptionally grave harm to national security" because it would risk informing adversaries of the nature and operational details of the process and scope of NSA's participation in the government's surveillance program.[168] On analysis of the government's assertion of the state secrets privilege, the court ultimately applied *Reynolds*' "reasonable danger" test, noting that it is not foreclosed under the holding in *Fazaga* and 50 U.S.C. § 1806(f) from still dismissing on state secrets grounds.[169]

The key difference between *Jewel* and *Fazaga* is whether the plaintiffs could demonstrate without discovery that they were "aggrieved," allowing the resolution of the case to be determined under FISA's procedures. The plaintiffs in *Fazaga* obtained information about their illegal surveillance from another case in which an FBI agent testified about Operation Flex and the government's use of electronic surveillance.[170] Since the plaintiffs had directly interacted with the FBI's informant involved in the operation,[171] and information about the operation had already been disclosed to the public,[172] they had more evidence to prove that they *themselves* were surveilled and qualified as "aggrieved."[173] The plaintiffs in *Jewel* had testimony of AT&T workers to prove their case,[174] but did not have sufficient evidence prior to discovery to prove that their *own* metadata was collected by the government.[175] It is therefore clear that while a plaintiff gets the protections of FISA if he or she is "aggrieved,"[176] the government may assert that the plaintiff lacks standing and thus does not qualify as "aggrieved," and then utilize the state secrets privilege to

165. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *40.
166. *See* 50 U.S.C. § 1806(f).
167. *Jewel*, 2019 U.S. Dist. LEXIS 217140, at *38.
168. *Id.* at *39–40.
169. *Id.* at *48–49.
170. Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1214 (9th Cir. 2019).
171. *Id.* at 1214.
172. *Id.*
173. *Id.* at 1254.
174. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *28–30.
175. *Id.* at *36.
176. *See generally Fazaga*, 916 F.3d at 1254.

deny the plaintiff evidence to demonstrate his or her standing and "aggrieved" status.[177]

Consequently, FISA's displacement of the state secrets privilege only provides additional privacy protection in cases where the plaintiff already has access to the evidence needed to prove that he or she is "aggrieved" under FISA.[178] As demonstrated in *Jewel*, FISA still runs into a roadblock of the state secrets privilege in cases where the plaintiff lacks such information, which results in plaintiffs' claims being denied based upon lack of standing.[179]

F. Safeguarding Americans Private Records Act (2020), USA Freedom Reauthorization Act (2020), and Protect Our Civil Liberties Act (2020)

In response to government surveillance abuse concerns, Congress recently introduced three major Acts intended to restore privacy and civil liberties.[180] First, Congress introduced the Safeguarding Americans Private Records Act ("SAPRA") which seeks to reform FISA.[181] Second, Congress introduced the USA Freedom Reauthorization Act ("FRA"), which attempts

177. *See generally Jewel*, 2019 U.S. Dist. LEXIS 217140, at *36.

178. *See generally Fazaga*, 916 F.3d at 1254.

179. *See generally Jewel*, 2019 U.S. Dist. LEXIS 217140, at *36.

180. *See generally* Justine Coleman, Massie, Gabbard team up on bill to repeal the Patriot Act, The Hill (Dec. 16, 2020, 1:50 PM), https://thehill.com/homenews/house/530498-massie-gabbard-team-up-on-bill-to-repeal-the-patriot-act [https://perma.cc/DMS4-NRKN] (describing the Protect Our Civil Liberties Act); Frank Konkel, *Bill Would Reform NSA Surveillance Program*, NEXTGOV (Jan. 27, 2020), https://www.nextgov.com/policy/2020/01/bill-would-reform-nsa-surveillance-program/162681/ [https://perma.cc/6ECV-7DLZ] (describing the Americans Private Records Act); Greg Nojeim & Mana Azarmi, *Revised USA FREEDOM Reauthorization Act of 2020 Improves FISA; More Improvements Are Needed*, CTR. FOR DEMOCRACY & TECH. (Mar. 11, 2020), https://cdt.org/insights/revised-usa-freedom-reauthorization-act-of-2020-improves-fisa-more-improvements-are-needed/ [https://perma.cc/ST9N-HVMA] (describing the USA Freedom Reauthorization Act).

181. S. 3242, 116th Cong. (2020). The Safeguarding Americans Private Records Act was introduced into Congress on January 28, 2020, and is still in the first stage of the legislative process. *See* GOVTRACK, S. 3242 (116th): Safeguarding Americans' Private Records Act of 2020 (Jan. 17, 2021), https://www.govtrack.us/congress/bills/116/s3242 [https://perma.cc/YPF5-WGJK]. This means that the Act still needs to be considered by a committee before it can be sent to the House or Senate. *Id.* The Act seeks to reform FISA by requiring that the government obtain a warrant before accessing location information, internet browsing, and search history; preventing the government from holding onto irrelevant records indefinitely; reforming the FISA court; and requiring more government transparency. S. 3242, 116th Cong. (2020).

to further amend FISA.[182] Third, Congress introduced the Protect Our Civil Liberties Act, which intends to repeal the United States Patriot Act and amend FISA.[183] However, none of these Acts address the standing problem that the state secrets privilege creates, or attempt to afford plaintiffs more judicial review in surveillance cases once they believe they have been wrongfully surveilled.[184] Instead, the Acts focus on proactively limiting use of government surveillance.[185]

III. CIRCUIT COURT SPLITS OVER THE STATE SECRETS PRIVILEGE

With the Supreme Court largely remaining quiet on the issue of the state secrets privilege in the nearly seven decades since *Reynolds* was decided, confusion has emerged amongst the circuit courts about how to apply and analyze the state secrets privilege in cases of electronic surveillance.[186] When the plaintiff has not established that he or she is "aggrieved" under FISA, the circuit courts all consistently return to applying the same three-part adaptation of the *Reynolds* "reasonable

182. H.R. 6172, 116th Cong. (2020). The USA Freedom Reauthorization Act was introduced into Congress on March 10, 2020, and has since been passed by the Senate with changes, and sent back to the House. *See* GOVTRACK, H.R. 6172: USA Freedom Reauthorization Act of 2020 (May 14, 2020), https://www.govtrack.us/congress/votes/116-2020/s92 [https://perma.cc/2QYK-QW57]. This Act similarly attempts to amend FISA as well as reauthorize it until December 2023. H.R. 6172, 116th Congress (2020). The Act states that the FBI cannot seek orders to obtain call records on an ongoing basis, cellular or GPS location information, or tangible things reasonably expected to be private and in which a warrant would typically be required. *Id.* Furthermore, the Act heightens requirements on FISA orders targeting a United States person or federal elected officials. *Id.*

183. H.R. 8970, 116th Cong. (2020). The Protect Our Civil Liberties Act was introduced into Congress on December 15, 2020, and is still in the first stage of the legislative process. Justine Coleman, *Massie, Gabbard team up on bill to repeal the Patriot Act*, THE HILL (Dec. 16, 2020, 1:50 PM), https://thehill.com/homenews/house/530498-massie-gabbard-team-up-on-bill-to-repeal-the-patriot-act. [https://perma.cc/66XQ-M5PY]. This Act seeks to repeal the United States Patriot Act and portions of the FISA Amendments Act that do not pertain to FISA court reporting and WMD intelligence collection. *Id.* It also provides protections for whistleblowers and requires heightened monitoring of federal intelligence agencies by the Government Accountability Office. *Id.*

184. *See generally* S. 3242, 116th Cong. (2020); H.R. 6172, 116th Cong. (2020); H.R. 8970, 116th Cong. (2020).

185. *See generally* S. 3242, 116th Cong. (2020); H.R. 6172, 116th Cong. (2020); H.R. 8970, 116th Cong. (2020).

186. *See generally* Herman, *supra* note 14, at 93–95.

danger" test.[187] However, the circuits have divided over how to apply this three-part test.[188]

Generally, to apply the *Reynolds* "reasonable danger" test, the court must first assess whether the procedural requirements for invoking the state secrets privilege have been satisfied.[189] Second, the court must decide whether the information sought to be protected qualifies as privileged under the state secrets privilege, assessing whether disclosure of the underlying documents or evidence would pose a reasonable danger to national security.[190] Finally, the court must determine how the matter should proceed in light of the successful privilege claim.[191] Lower courts have identified some examples of circumstances in which the privileged information is so central to the litigation that there is a reasonable danger that proceeding with the case will endanger national security and dismissal is required.[192] First, dismissal is required if the plaintiff cannot prove the *prima facie* elements of his or her claim without privileged evidence; second, even if the plaintiff can prove a *prima facie* case without resorting to privileged information, the case should be dismissed if the defendants could not properly defend themselves without using privileged evidence; and third, dismissal is appropriate where further litigation would present an unjustifiable risk of disclosure of state secrets.[193]

While there are other areas of division among the circuit courts over the state secrets privilege,[194] the most important division is over the

187. *See* Ibrahim v. U.S. Dep't of Homeland Sec., 912 F.3d 1147, 1164 (9th Cir. 2019); Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081 (9th Cir. 2010); Sec. and Exch. Comm'n v. Schroeder, No. C07-03798JW, 2008 U.S. Dist. LEXIS 46465, at *5–6 (N.D. Cal. Jan. 15, 2008).

188. *See generally* Herman, *supra* note 14, at 93–95.

189. United States v. Reynolds, 345 U.S. 1, 9 (1953).

190. *Id.* at 10.

191. *Id.*

192. *See* Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., 427 F. Supp. 3d 582, 612 (D. Ct. Md. 2019).

193. *Id.*

194. For example, one area of division is between the Ninth and Fourth Circuit, over where the privilege originates and whether it has a firm basis in the Constitution. *See* El-Masri v. United States, 479 F.3d 296, 303–05 (4th Cir. 2007); *cf.* Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1230–31 (9th Cir. 2019). This division has impacted the Circuit Court approaches to analyzing state secrets privilege claims, with the Fourth Circuit consistently ruling in favor of the privilege and affording the executive branch extreme deference (*see El-Masri*, 479 F.3d at 303–04), while the Ninth Circuit questions the privilege's viability in modern-day society (*see Fazaga*, 916 F.3d at 1230). The Fourth Circuit adopts a very broad and favorable reading of the state secrets privilege, and is hesitant to rule against a claim of state secrets privilege, finding that the privilege has a firm foundation in the Constitution in addition to its basis in the common law of evidence (*see, e.g.*, Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., 427 F. Supp. 3d 582, 610

third-prong of the *Reynolds* test, which requires the court to determine how the matter should proceed in light of the successful privilege claim.[195] The division is over whether the state secrets privilege requires dismissal of an entire claim if the case could potentially expose issues that implicate state secrets, or whether the court may instead exclude just the specific privileged evidence and allow the claim to continue.[196] The D.C. Circuit evaluates whether the claim may proceed using alternative evidence, or by "disentangling the non-sensitive information" before dismissing the case.[197] Conversely, the Fourth and Ninth Circuits dismiss cases without considering alternatives to substitute for the privileged evidence.[198] This division has contributed to the current problem with the state secrets privilege, leading to more judicial deference to the executive from the Fourth and Ninth Circuits to avoid overstepping into matters outside of judicial jurisdiction, and consequently, more electronic surveillance cases being dismissed for lack of standing.

(D. Ct. Md. 2019)), whilst the Ninth Circuit interprets it narrowly and has shifted towards curtailing widespread use of the privilege, finding its basis only in the common law and not in the Constitution (*see Fazaga*, 916 F.3d at 1230–31). Note that a second Circuit Court split also exists over how to apply *Reynolds*' "reasonable danger" test with regard to the second-prong of the analysis. The Fourth and Ninth Circuits have taken the view that the *Reynolds'* "reasonable danger" test is composed of just the original three-part test from *Reynolds*. *See El-Masri*, 479 F.3d at 311; *see also* Jewel v. Nat'l Sec. Agency, No. C 08-04373 JSW**,** 2019 U.S. Dist. LEXIS 217140, at *48–49 (Cal. D. Ct. Apr. 25, 2019). The D.C. Circuit, however, has added an additional requirement to the second part of the test: once the court decides that the evidence or documents would pose a reasonable danger to national security and the privilege is thus properly invoked, the court must then conduct an additional balancing test, weighing the harm of disclosing the evidence to national security with the harm that would be caused by withholding the evidence from the plaintiff. Halkin v. Helms (Halkin II), 690 F.2d 977, 990 (D.C. Cir. 1982).

195. *See Jewel*, 2019 U.S. Dist. LEXIS 217140 at *48–49. *See generally El-Masri*, 479 F.3d at 306; Ellsberg v. Mitchell, 709 F.2d 51, 57 (11th Cir. 1983); Farnsworth Cannon, Inc. v. Grimes, 635 F.2d 268, 273 (4th Cir. 1980).

196. *See El-Masri*, 479 F.3d at 306; *Farnsworth Cannon, Inc.*, 635 F.2d at 273; s*ee also Jewel*, 2019 U.S. Dist. LEXIS 217140 at *48–49; *Ellsberg*, 709 F.2d at 57.

197. *Ellsberg*, 709 F.2d at 57.

198. *See El-Masri*, 479 F.3d at 311; *see also Jewel*, 2019 U.S. Dist. LEXIS 217140, at *48–49.

IV. GOVERNMENT SURVEILLANCE OF INDIVIDUALS

A. New Surveillance Technologies

With ever increasing technological advancements, new surveillance capabilities have likewise followed.[199] In 2019, the United States Department of Defense launched solar-powered surveillance balloons known as Stratollites across six states with the goal of testing a persistent surveillance system that can locate and detect narcotic trafficking and homeland security threats.[200] The balloons carry hi-tech radars that simultaneously track vehicles and boats all day and night.[201] Such tests have been commissioned by the United States Southern Command, responsible for identifying and intercepting drug shipments headed for the United States.[202]Although the balloons serve the purpose of detecting narcotic trafficking and homeland security threats, they incidentally collect a vast amount of data on Americans, essentially surveilling every vehicle on the road.[203] Stratollites are not a new phenomenon.[204] A Stratollite company named World View has been around since 2012, and began using their Stratollites as a data services platform as early as 2014.[205] World View started-out using their technology to collect high-resolution images of Earth and selling this data to the government and private companies, but has indicated that it would start selling its data to the United States Department of Defense in 2020.[206] Considering that World View's system is capable of detecting whether a person on the ground is "holding a shovel or a gun,"[207] it is certainly concerning what this will mean for individual privacy rights.

Surveillance technology has also made its way into homes in recent years. Perhaps unsurprisingly, such devices can and do collect data from Americans in the privacy of their own homes.[208] For example, Google

---

199. *See generally* White, *supra* note 125.

200. Mark Harris, *Pentagon Testing Mass Surveillance Balloons across the US*, THE GUARDIAN (Aug. 2, 2019), https://www.theguardian.com/us-news/2019/aug/02/pentagon-balloons-surveillance-midwest?CMP=share_btn_tw [https://perma.cc/DT5L-AEG3].

201. *Id.*

202. *Id.*

203. *Id.*

204. *See generally* Daniel Oberhaus, *Giant Surveillance Balloons Are Lurking at the Edge of Space*, WIRED (Dec. 19, 2019, 12:27 AM), https://www.wired.com/story/giant-surveillance-balloons-are-lurking-at-the-edge-of-space/ [https://perma.cc/T25Y-6SZZ].

205. *Id.*

206. *Id.*

207. *Id.*

208. Carol Nackenoff, *"Only the Beginning, Only Just the Start . . . Mostly I'm Silent": New Constitutional Challenges with Data Collection Devices Brought into the Home*, 79 MD. L. REV. 88, 90 (2019).

Home collects data on all Google Assistant queries, whether audio or typed, and collects the location where the query occurred.[209] Yet Google Home is just one of many artificial intelligence devices that people bring into the home: Alexa, Siri, and Cortana are other devices commonly used in the home.[210] Outside of the home, surveillance technology follows in the form of a smart car, FitBit, and smartphones.[211] Each of these devices produce a colossal amount of data which is collected and stored by the private companies that own such devices, but that is potentially subject to access by the government.[212] In fact, since 9/11, the government has become increasingly dependent on the private sector for national security purposes, and government demands for data held by the private sector have increased.[213]

Recently, in response to the COVID-19 pandemic, the United States began digital contact tracing in an attempt to lower the spread of COVID-19.[214] Apple and Google have implemented mobile applications that cross-check the user's data history to see if they have been in close proximity to someone who has been diagnosed with COVID-19.[215] When someone officially tests positive for COVID-19 the system can send a notification to anyone who was recently near that person, telling them to contact their local health authority and get medical advice and a test.[216] However, a recent study of fifty COVID-19 related applications has revealed that thirty of the fifty applications require permission for access to contacts, photos, media, files, location data, camera, device identification, Wi-Fi connection, microphone, full network access, Google service configuration, and the ability to change network connectivity and audio

209. *Id.*

210. *Id.* at 88.

211. *Id.*

212. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/8SDF-6GH7].

213. *See generally id.*

214. TJ McCue, *iPhone And Android App For COVID-19 Contact Tracing Will Be Strictly Opt-In Only*, FORBES (Apr. 24, 2020, 11:10 PM), https://www.forbes.com/sites/tjmccue/2020/04/24/iphone-and-android-app-for-covid-19-contact-tracing-will-be-strictly-opt-in-only/?sh=59ff22725a32#71cf6ecb5a32 [https://perma.cc/Q5AR-JHPM].

215. *Id.*

216. Kif Leswing, *Three States Will Use Apple-Google Contact Tracing Technology for Virus Tracking Apps*, CNBC (May 20, 2020, 5:37 PM), https://www.cnbc.com/2020/05/20/three-states-commit-to-apple-google-technology-for-virus-tracking-apps.html [https://perma.cc/3U98-YM5S].

settings.[217] Some of the applications also state that they will collect information about the user's age, email address, phone number, zip code, the device's location, unique device identifiers, mobile IP address, and the types of browsers used on the mobile device.[218] Furthermore, only sixteen of the fifty applications indicate that the user's data will be made anonymous, encrypted, and secured.[219] The study noted that at least three applications developed by United States healthcare providers have similar functionalities, including Sentinel Healthcare, 98point6, and HealthLynked.[220] Although it is not mandatory for Americans to download and use these applications, privacy concerns arise over people using the applications without understanding the vast amount of data being collected from them and without yet knowing how their data will be used by the government.[221] It is therefore clear that current and emerging technologies and society's increasing dependence on technology subjects the public to more potential surveillance abuses, and indicates that it is becoming more important for plaintiffs to be able to litigate surveillance cases against the government.

B. The Third-Party Doctrine

Perhaps the most concerning aspect of current government surveillance is the intersection between the use of technology when an individual interacts with another private party, corporate or otherwise, and the Fourth Amendment's third-party doctrine.[222] The third-party doctrine is the general rule that when an individual discloses information to a third-party, he or she forfeits any Fourth Amendment privacy rights over that information.[223] Thus, when the government acquires previously obtained information about an individual from a third-party, the third-party doctrine applies and the government is not deemed to be performing a Fourth Amendment search of that individual.[224] The third-party doctrine therefore makes it constitutional for the government to acquire information about an

---

217. Tanusree Sharma & Masooda Bashir, *Use of Apps in the COVID-19 Response and the Loss of Privacy Protection*, NATURE MED. (May 26, 2020), https://www.nature.com/articles/s41591-020-0928-y [https://perma.cc/QHG9-QPGS].

218. *Id.*

219. *Id.*

220. *Id.*

221. *See id.*

222. *See generally* Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. L. REV. 1441 (2017).

223. *See* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 110–11 (2018).

224. *Id.*

individual that was originally obtained by a third-party, and legal for the third-party to voluntarily or involuntarily hand-over such information to the government.[225]

The third-party doctrine began to emerge as early as 1952, developing throughout a series of cases establishing the general principle that people who mistakenly confide their crimes to undercover police or informants have assumed the risk of betrayal.[226] *United States v. Miller* extended the third-party doctrine to apply not only to in-person conversations, but also to business records.[227] Therein, the Supreme Court stated that the government's issuance of a subpoena to a third-party to obtain records of a defendant does not violate the constitutional rights of a defendant.[228] The records being obtained in *Miller* were bank records, and the court held that there was no legitimate expectation of privacy in records of checks and deposit slips since they are information voluntarily conveyed to banks.[229] The court noted that the Fourth Amendment does not prohibit obtaining information revealed or conveyed to a third-party, even when such conveyance was made on the understanding that the communication is confidential.[230] In other words, even if a consumer shares their information with a corporation believing and agreeing that it will be kept confidential, he or she cannot object if the third-party thereafter conveys that information to law enforcement authorities.[231] Thus, whether communication between a private citizen and a third-party is confidential or not, the third-party may hand over such information to the government upon request.[232]

Furthermore, *Miller* has indicated that not only does the third-party doctrine apply to voluntary surrender of such information by a third-party, it also applies where the government forces the surrender of information held by the third-party, for example through the use of a subpoena.[233] So even if a third-party does not agree to hand over data to the government, it may nevertheless be forced to do so.[234] The third-party doctrine has since been solidified in cases such as *Smith v. Maryland*, when the Supreme Court held that a person has no legitimate expectation of privacy in the information he voluntarily turns over to third-parties.[235]

---

225. *See generally* Richards, *supra* note 222.
226. *See generally id.* at 1467.
227. *Id.* at 1468–69.
228. United States v. Miller, 425 U.S. 435, 444 (1976).
229. *Id.* at 442.
230. *Id.* at 443.
231. *See* Sec. and Exch. Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).
232. *Id.*
233. *Miller*, 425 U.S. at 444.
234. *Id.*
235. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

With the rise of technology, records once stored in paper format have progressively moved online, to the point where so much data is stored that it is becoming difficult to quantify.[236] The third-party doctrine permits the government to access a vast array of information about individuals, including websites they visit, who they email, phone numbers they dial, utility records, banking records, and education records, to name just a few.[237] The third-party doctrine has been used extensively by the National Security Agency ("NSA") to collect such information from private companies. [238] The NSA is a government agency that collects and processes foreign communications for intelligence and counterintelligence.[239] Unfortunately, the NSA does not have a clean record.[240] In 2013, Edward Snowden, a former NSA contractor, revealed to the public a program named "PRISM" in which the NSA bulk-collected United States citizens' phone records without a warrant.[241] Snowden leaked a FISC order to the British newspaper *The Guardian* that directed the telephone company Verizon to produce to the NSA call detail records, every day, on *all* telephone calls made through its systems or using its services where one or both ends of the call are located in the United States.[242] After the order was published, the government acknowledged that it was part of a broader program of bulk collection of telephone metadata from other telecommunications providers too.[243] It soon came to light that the NSA additionally collected private electronic data belonging to users of

---

236. *See* Charles Walford, *Information overload: There is so much data stored in the world that we may run out of ways to quantify it*, DAILY MAIL (Dec. 12, 2012, 12:55 PM), https://www.dailymail.co.uk/sciencetech/article-2247081/There-soon-words-data-stored-world.html [https://perma.cc/L9TN-QRHP].

237. RICHARD M. THOMPSON II, CONG. RSCH. SERV., REP. NO. 43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014).

238. *See generally* Spy Shelter, *A Journey Through Interesting NSA Surveillance Programs*, SPY SHELTER (June 11, 2014), https://www.spyshelter.com/blog/a-journey-through-interesting-nsa-surveillance-programs/ [https://perma.cc/3X3N-T2TD].

239. Lauren Doney, *NSA Surveillance,* Smith *& Section 215: Practical Limitations to the Third-Party Doctrine in the Digital Age*, 3 NAT'L SEC. L.J. 462, 463–64 (2015).

240. *See generally* Corinne Reichert & Laura Hautala, *Appeals Court Finds NSA's Bulk Phone Data Collection Was Unlawful*, CNET (Sept. 2, 2020, 3:02 PM), https://www.cnet.com/news/appeals-court-finds-nsas-bulk-phone-data-collection-was-unlawful/ [https://perma.cc/72P2-WB3C].

241. *Id. See also* T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013, 1:36 PM), https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet [https://perma.cc/QK6D-DFEB].

242. ACLU v. Clapper, 785 F.3d 787, 796 (2d Cir. 2015).

243. *Id.* at 796.

platforms such as Gmail, Facebook, and Outlook.[244] Under the third-party doctrine, the NSA was able to request phone records from companies like AT&T and Verizon,[245] and collect data on specific people from major technology companies like Google, Yahoo, Facebook, Microsoft, and Apple.[246] In recent years, lawsuits have consistently been brought against the government for the NSA's past abuses of data collection and usage.[247] On September 2, 2020, the Ninth Circuit indicated that the government violated FISA and may have also violated the Fourth Amendment when it collected the telephony metadata of millions of Americans through the NSA.[248] Thus, PRISM was illegal and potentially a violation of constitutional rights.[249] Although there has yet to be any news of additional NSA abuses over the past few years, PRISM set the stage for current concerns over social media giants like Facebook giving data to the government.[250]

In 2013, following revelations about Facebook's co-operation with the NSA's mass surveillance of United States and foreign citizens, Facebook began releasing information to the public about government requests for information.[251] In the first half of 2013, the government requested information on 20,000 Facebook users.[252] The government made 11,000 requests for information about these individuals, and Facebook

244. Sottek & Kopfstein, *supra* note 241.

245. Phil Goldstein, *Reports: NSA Gets Phone Records from Verizon, AT&T, Sprint, as Well as Data from Apple, Google, and Others*, FIERCE WIRELESS (Jun. 7, 2013, 11:03 AM), https://www.fiercewireless.com/wireless/reports-nsa-gets-phone-records-from-verizon-at-t-sprint-as-well-as-data-from-apple-google [https://perma.cc/7BCN-ASTB].

246. Sottek & Kopfstein, *supra* note 241.

247. *See* United States v. Moalin, 973 F.3d 977, 984–86 (9th Cir. 2020). *See also* Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., 857 F.3d 193, 200 (4th Cir. 2017); ACLU v. Nat'l Sec. Agency, 493 F.3d 644, 648 (6th Cir. 2007); Agility Pub. Warehousing Co. K.S.C. v. Nat'l Sec. Agency, 113 F.Supp. 3d 313, 318 (D.D.C. 2015).

248. *Moalin*, 973 F.3d at 993.

249. *See generally id.*

250. *See* Kalev Leetaru, *Facebook As The Ultimate Government Surveillance Tool?*, FORBES (July 20, 2018, 3:15 PM), https://www.forbes.com/sites/kalevleetaru/2018/07/20/facebook-as-the-ultimate-government-surveillance-tool/?sh=12dbb5542909 [https://perma.cc/8PJW-EEA8].

251. Dominic Rushe, *Facebook Reveals Governments Asked for Data on 38,000 Users in 2013*, THE GUARDIAN (Aug. 28, 2013, 3:49 PM), https://www.theguardian.com/technology/2013/aug/27/facebook-government-user-requests [https://perma.cc/94ZE-T24W].

252. Transparency Center, *Government Requests for User Data*, FACEBOOK, https://transparency.fb.com/data/government-data-requests/country [https://perma.cc/NJK2-UCRZ] (last visited Aug. 1, 2021) (Select the time period "Jan-Jun 2013" then choose "United States").

complied in 79% of cases.[253] By the second half of 2019, the government made 51,121 requests on 82,321 user accounts, and Facebook complied with 88% of cases.[254] In order to comply, Facebook requires a subpoena, a court order, or a search warrant, but does not seek out the individual's consent before handing-over information.[255] The number of requests made by the government to Facebook has increased significantly over the years, with an 88% compliance rate at the end of 2019.[256]

Throughout the COVID-19 pandemic, the population's reliance on technology has only increased.[257] The videoconferencing company, Zoom, has had its daily number of users increase from ten million in 2019, to 200 million users in March 2020.[258] Zoom collects a huge amount of data on its users, including name, email, phone number, billing information, location data, IP address, and much more from information in administrator accounts.[259] Since Zoom has only recently increased in popularity, there has yet to be any information released to the public on the amount of government requests for its users' information.[260] However, Zoom has created similar guidelines to Facebook for compliance with requests, including the requirement of a subpoena, court order, or a search warrant, and not an individual's consent before handing-over information.[261] Facebook's trend toward releasing its users' information to the government, along with the United States' increased reliance on technology companies that inevitably collect data on individuals, indicate that the third-party doctrine is potentially obliterating any expectation of privacy otherwise possessed by individuals under the Fourth Amendment.[262]

---

253. *Id.*

254. *Id.*

255. Facebook Safety Center, *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ [https://perma.cc/RK5Z-VR23] (last visited Aug. 1, 2021).

256. Transparency Center, *supra* note 252 (Select the time period "Jul-Dec 2019" then choose "United States").

257. Nina J. Ginsberg, *Third-Party Doctrine in the Age of COVID-19*, NACDL (Aug. 28, 2020), https://nacdl.medium.com/third-party-doctrine-in-the-age-of-covid-19-876ba9c8cb8a [https://perma.cc/K7DB-BSEX].

258. *Id.*

259. *Zoom Privacy Statement*, ZOOM, https://zoom.us/privacy/ [https://perma.cc/C9ME-GDVH] (last visited Aug. 1, 2021).

260. *See generally Government Requests Guide*, ZOOM, https://zoom.us/docs/en-us/government-requests-guide.html [https://perma.cc/9YQY-QEWE] (last visited Aug. 1, 2021) (showing that, while there is information provided about governmental requests, there is no information regarding the number of such requests).

261. *Id.*

262. Ginsberg, *supra* note 257.

Supreme Court Justices have begun questioning the continuing viability of the third-party doctrine based on current social realities.[263] Justice Sotomayor has stated that the third-party doctrine is ill-suited to the digital age because nowadays, people reveal a great deal of information about themselves to third-parties in the course of carrying-out just simple mundane tasks.[264] Justice Gorsuch has also expressed his concerns with the third-party doctrine, explaining that private documents that used to be locked safely in a desk drawer are now stored on third-party servers, and can be reached and reviewed in-full by police.[265] He has also suggested that users may have a property interest in cell phone records stored by third-parties.[266] However, the third-party doctrine has yet to be reformed to deal with expansive technology in the digital age.[267]

C. Carter Page FISA Abuses

Following claims of spying on the Trump campaign and the FISC's subsequent declassified ruling on FISA abuses pertaining to Carter Page, a foreign policy advisor to then presidential candidate Donald Trump,[268] it has become widespread knowledge that FISA procedures are not consistently followed by the FBI.[269] In its June 2020 ruling, the FISC indicated that it approved four applications by the government in 2016 and 2017 to electronically surveil and physically search target Page pursuant to FISA.[270] The government sought to investigate Page due to his prior contacts with known Russian intelligence officers, but had insufficient

263. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring); Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

264. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring).

265. *Carpenter*, 138 S. Ct. at 2262.

266. *Id.*

267. *See generally* Richards, *supra* note 222, at 1488.

268. *See generally* James Bovard, *Inspector General Report on FBI's FISA Abuse Tells Us One Thing: We Need Radical Reform*, USA TODAY (Dec. 10, 2019, 1:38 PM), https://www.usatoday.com/story/opinion/2019/12/10/ig-report-fbi-fisa-abuse-secret-court-trump-campaign-column/4383722002/ [https://perma.cc/2C2Q-L3BK].

269. *See* Jordan Davidson, *FISA Court Confirms The Government Lied In Every Spy Warrant Application Against Carter Page*, THE FEDERALIST (Sep. 17, 2020), https://thefederalist.com/2020/09/17/fisa-court-confirms-the-government-lied-in-every-spy-warrant-application-against-carter-page/ [https://perma.cc/LA5S-JUBW]. *See generally* Bovard, *supra* note 268.

270. In re Carter W. Page, Nos. 16-1182, 17-52, 17-375, 17-679, at 1 (FISA Ct. Jan 7, 2020).

probable cause to do so.[271] Cristopher Steele, a former British intelligence officer, was hired by Fusion GPS to conduct research on Page on behalf of the Democratic National Committee and the Hillary Clinton presidential campaign.[272] Steele created a dossier later found to be based on rumor and speculation.[273] Steele forwarded his political opposition research to the FBI, and the FBI relied on Steele's dossier to engage FISA to monitor Page.[274] In its June 2020 ruling, the FISC court noted that the government made material errors and omissions in the FISA applications, fabricating that there was probable cause to believe that Page was an agent of a foreign power.[275] The government admitted that at least two of its applications lacked factual support,[276] and the court indicated that FISA procedures were improperly followed by the government, and that the information on Page was obtained through unlawful surveillance and search.[277]

The abuses committed by FISA in illegally obtaining information on Page have revealed vulnerability of FISA to disinformation, and indicate potential politicization of FISA.[278] The investigation of the Page FISA applications indicated that the FBI "drew almost entirely from Steele's reporting" and that the Steele Dossier was "central and essential" to securing FISA surveillance of Page.[279] Yet the FBI knew that Steele was an unreliable source and omitted such information in the FISA applications, which indicates that the FBI knew or should have known that they were likely including misinformation on their applications.[280] The FISA warrant on Page was subsequently renewed at a time when it had been confirmed to the government that Steele was working for Clinton and wanted to prevent Trump's election.[281] The Investigator's report on the FISA applications for Page indicate politicization of FISA, noting that messages between parties involved, including the FBI's Chief of Counter-Espionage and Deputy Assistant Director, implied action on the basis of political sentiments, and may help account for the FBI's FISA errors.[282] The FBI were essentially investigating Page based on their own political feelings about Trump, and

---

271. OFFICE OF THE INSPECTOR GENERAL, U.S. DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019).

272. *See* Bernard Horowitz, *FISA, The "Wall," and Crossfire Hurricane: A Contextualized Legal History*, 7 NAT'L SEC. L J. 1, 80–81 (2019).

273. *See generally id*. at 81.

274. *Id.* at 82–83.

275. In re Carter W. Page, Nos. 16-1182, 17-52, 17-375, 17-679, at 1 (FISA Ct. Jan 7, 2020).

276. *Id.* at 4.

277. *Id.* at 8.

278. *See* Horowitz, *supra* note 272, at 93–98.

279. *Id.* at 84–85.

280. *Id.* at 86–87.

281. For a detailed account of subsequent FISA renewals, see *id.* at 89–90.

282. *Id.* at 92–93.

failed to instead question the sources of their information as they would do normally.[283]

The Page FISA abuses offer an illustration of FISA surveillance applications that are flawed, placing civil liberties at risk.[284] It is now clear that in reviewing and approving FISA applications, courts only look to whether the FBI followed the correct procedures in filing the applications instead of questioning what substantive information the FBI puts on the applications.[285] FISA surveillance is thus only safeguarded by the procedures the FBI must follow in obtaining a FISA warrant and a determination of whether they followed such procedures, as opposed to what they actually put on each application as cause for a FISA warrant.[286] Yet all stages of the FISA procedures rely heavily on what the FBI tells the Office of Intelligence ("OI"), and the OI's scrutiny is limited.[287] Moreover, the Carter Page FISA applications indicate that the FBI may be relying on misinformation and political bias in securing its FISA warrants.[288] FBI FISA practitioners have also indicated that FISA judges "don't know what to look for" when reviewing FISA applications.[289] Without scrutiny from the OI or the judiciary, the FBI is currently given next to unchecked power when it comes to obtaining a FISA warrant.[290]

D. Legislation Strengthening Government Surveillance Powers

In addition to the FISA Amendments Reauthorization Act mentioned in Section III, government surveillance powers have continued to increase through various other enacted legislation, paving the way for more potential surveillance abuses and contributing to the current problem with the state secrets privilege.[291] Government surveillance powers surged after 9/11 in response to national security concerns.[292] In 2001, Congress enacted the U.S. Patriot Act.[293] The Patriot Act strengthened dragnet government surveillance,[294] and allowed the CIA to access information on United States citizens such as phone and email communications, internet use, bank and credit reporting records, school records, and details of

283. *See generally id.* at 93–95.
284. *See generally id.*
285. *Id.* at 98.
286. *Id.*
287. *Id.* at 102.
288. *See generally id.* at 93–95.
289. *Id.* at 103.
290. *See generally id.* at 93–95.
291. *See generally* Ker, *supra* note 63.
292. *Id.*
293. The Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.
294. *Id.*

criminal investigations and grand jury proceedings.[295] Two years later, the government conducted project Stellarwind, which allowed the NSA to monitor call and text metadata of United States citizens and tap any international calls that included a United States caller without a warrant.[296] The NSA did not claim to have ended Stellarwind until 2019.[297] Projects PRISM and Upstream also followed Stellarwind in 2007.[298] PRISM allows the NSA to collect private internet data of foreign nationals, but incidentally swept up data of United States citizens in the process.[299] Such data includes emails, files, photos, and user accounts on Gmail, Facebook, Apple, and Microsoft.[300] Upstream supports PRISM by infiltrating the infrastructure of the internet to copy and filter its traffic.[301] However, unlike Stellarwind, it is unclear whether PRISM and Upstream are still active programs.[302]

In 2013, Edward Snowden, a former NSA contractor, revealed surveillance abuses under the NSA which pressured a reform of the Patriot Act.[303] The U.S. Freedom Act of 2015 reauthorized parts of the Patriot Act but also dissolved NSA's bulk collection of United States citizens' phone records and internet metadata.[304] However, the NSA still collected a total of 695 million call-detail records between 2016 and 2017 under the Freedom Act. Also, in 2018 it was revealed that due to technical irregularities, the NSA had possession of vast amounts of detailed call records and metadata that it had no authority to receive.[305] The Freedom Act was sought to be reauthorized in 2020, but lost support from the president and congressmen and was ultimately taken off the floor.[306]

---

295. Ker, *supra* note 63.

296. Shane Harris, *Confessions from Bush's NSA Spy Program*, DAILY BEAST (updated July 12, 2017, 6:34 PM), https://www.thedailybeast.com/confessions-from-bushs-nsa-spy-program. [https://perma.cc/C5RP-2CCS].

297. Ker, *supra* note 63.

298. *Id.*

299. *Id.*

300. *Id.*

301. *Id.*

302. Laura Hautala, *NSA surveillance programs live on, in case you hadn't noticed*, CNET (Jan. 19, 2018, 11:25 AM), https://www.cnet.com/news/nsa-surveillance-programs-prism-upstream-live-on-snowden/ [https://perma.cc/QZ3T-447G].

303. Ker, *supra* note 63.

304. *USA Freedom Act: What's in, what's out*, WASH. POST (Jun. 2, 2015), https://www.washingtonpost.com/graphics/politics/usa-freedom-act/ [https://perma.cc/8PZA-2AVE].

305. Ker, *supra* note 63.

306. Nicholas Fearn, *Patriot Act surveillance powers left unrenewed after Trump threatens veto*, TOM'S GUIDE (May 29, 2020), https://www.tomsguide.com/news/fisa-provisions-die-in-house [https://perma.cc/W6DG-5BWA].

V. CURRENT PROBLEM WITH THE STATE SECRETS PRIVILEGE

Even though FISA is designed to create some protection against improper government surveillance of private citizens, *Jewel* has demonstrated that the state secrets privilege will likely prevent plaintiffs from benefiting from its protections because they cannot demonstrate that they are "aggrieved" under FISA.[307] With the government claiming state secrets privilege prior to discovery on the issue of standing, plaintiffs cannot obtain the evidence they need from the government to prove that they themselves were victims of illegal surveillance, and thus cannot show that they are "aggrieved" or that they have standing to bring the case.[308] Courts then return to applying the common law *Reynolds* "reasonable danger" test, and electronic surveillance cases are dismissed before the plaintiff has a chance to reach the merits of his or her claim.[309]

A plaintiff's inability to obtain evidence needed to prove his or her standing presents numerous constitutional and policy problems when such evidence is held in privilege by the government. There are three major constitutional concerns that arise as a result of standing being denied behind a cloak of the state secrets privilege. These include unrestrained violations of Fourth Amendment rights to be secure in one's person, houses, papers, and effects, against unreasonable searches and seizure;[310] First Amendment rights to freedom of speech, association, and religion;[311] and Fifth Amendment rights to equal protection of the law.[312] Additionally, there are at least two significant public policy problems that arise as a result of the state secrets privilege being used to deny standing.[313] These include the undermining of privacy protections and a basic sense of justice in the United States.[314]

---

307. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *48–49 (N.D. Cal. Apr. 25, 2019); *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

308. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *47–48.

309. *See* Ibrahim v. United States Dep't of Homeland Sec., 912 F.3d 1147, 1164 (9th Cir. 2019); Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081 (9th Cir. 2010); Sec. and Exch. Comm'n v. Schroeder, No. C07-03798JW, 2008 U.S. Dist. LEXIS 46465, at *13–14 (N.D. Cal. Jan. 15, 2008).

310. *See* U.S. CONST. amend. IV.

311. *See* U.S. CONST. amend. I.

312. *See* U.S. CONST. amend. V.

313. *See e.g.*, United States v. Moalin, 973 F.3d 977, 987 (9th Cir. 2020) (indicating that the United States' collection of telephonic metadata potentially violates the Fourth Amendment); Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1212–13 (9th Cir. 2019) (reasoning that government surveillance potentially violates the First and Fifth Amendments and that the inability to litigate electronic surveillance cases due to the state secrets privilege provides the government with an unchecked power).

314. *Id.*

A. Constitutional Violations

The state secrets privilege undermines constitutional rights on two levels. First, the government may be committing constitutional violations by illegally surveilling the plaintiff, and second, constitutional concerns arise in response to the plaintiff's inability to litigate his or her case when he or she reasonably suspects that wrongful surveillance has occurred.

There are three main constitutional concerns that arise from illegal government surveillance itself. First, current government surveillance may be a Fourth Amendment violation of the right to be secure in one's person, houses, papers, and effects, against unreasonable searches and seizure.[315] The court has already ruled that one of the government's surveillance programs, NSA's bulk collection of metadata (which was part of PRISM), is likely a Fourth Amendment violation because it violated the right to a reasonable expectation of privacy.[316] Second, government surveillance is likely a First Amendment violation of the right to freedom of speech, association, and religion in cases involving government surveillance of individuals based solely on their religion or who they are associated or communicate with.[317] Third, government surveillance could be a Fifth Amendment violation of the right to equal protection in cases where the individual is a target of surveillance solely because of their race or ethnicity, without a compelling government interest and the least restrictive means used to achieve that interest.[318]

Additionally, the inability to litigate an electronic surveillance case likely undermines the constitutional system of checks and balances because the state secrets privilege is currently functioning as almost an absolute and unchecked privilege for the executive branch.[319] Furthermore, a plaintiff's inability to litigate is likely a violation of the Fifth Amendment right to not be deprived of life, liberty, or property without due process of the law.[320] This violation is implicated because the state secrets privilege is insulating government surveillance programs from judicial scrutiny, undermining the due process rights of individuals harmed by the programs.[321]

---

315. U.S. CONST. amend. IV.

316. *See Moalin*, 973 F.3d at 989.

317. *See, e.g.*, *Fazaga,* 916 F.3d at 1212–13.

318. *See, e.g.*, *id.*

319. *See* ACLU, *ACLU Statement to the House Judiciary Committee on the Use of the State Secrets Privilege* (Jan. 29, 2008), https://www.aclu.org/other/aclu-statement-house-judiciary-committee-use-state-secrets-privilege [https://perma.cc/DBE6-U3JC].

320. U.S. CONST. amend. V.

321. *See generally* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *48–49 (N.D. Cal. Apr. 25, 2019).

First, wrongful government surveillance of individuals could constitute a Fourth Amendment violation.[322] The Fourth Amendment guarantees the right to be secure in one's person, houses, papers, and effects, against unreasonable searches and seizure.[323] It also provides that a warrant shall not be issued without probable cause and unless supported by Oath or Affirmation, and particularly describing the place to be searched and the persons or things to be seized.[324] One way in which the Fourth Amendment has been interpreted by the courts is as a protection of one's reasonable expectation of privacy.[325] For such protections to be invoked, a plaintiff must show he or she had an actual, subjective expectation of privacy and that the expectation is one that society is prepared to recognize as reasonable.[326]

An obvious example of a reasonable expectation of privacy is that expected in one's own home.[327] Yet the widespread use of devices in the home that could be monitored by the government places Fourth Amendment rights at risk.[328] For example, the Ninth Circuit held in *Moalin* that NSA's bulk collection of United States citizens' telephony metadata under PRISM may have been a violation of the Fourth Amendment right to be secure against unreasonable searches and seizures.[329] Presumably, a majority of these phone calls were made with the reasonable expectation that they would be private, and some likely occurred whilst the caller or receiver was at home.[330] The court explained that technological advances throughout the years have enabled the government to collect and analyze information about its citizens on an unprecedented scale, splintering Fourth Amendment rights.[331] The court held that NSA's metadata collection may have been a Fourth Amendment violation because it included much more comprehensive communications than cases in the past,[332] the duration and

322. *See generally* United States v. Moalin, 973 F.3d 977, 989 (9th Cir. 2020).

323. U.S. CONST. amend. IV.

324. *Id.*

325. Derek M. Alphran, *Changing Tides: A Lesser Expectation of Privacy in a Post 9/11 World*, 13 RICH. PUB. INT. L. REV. 89, 90 (2009).

326. *Moalin,* 973 F.3d at 989 (quoting Katz v. United States, 389 US 347, 361 (1967) (Harlan, J., concurring)).

327. *See* United States v. Kyllo, 533 U.S. 27, 37 (2001); FINDLAW, *What Is the "Reasonable Expectation of Privacy"?*, (July 17, 2017), https://www.findlaw.com/injury/torts-and-personal-injuries/what-is-the--reasonable-expectation-of-privacy--.html [https://perma.cc/BYH3-6663].

328. Dorian Lynskey, *"Alexa, are you invading my privacy?"- the dark side of our voice assistants*, THE GUARDIAN (Oct. 9, 2019, 1:00 PM), https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants [https://perma.cc/H2HY-3TPB].

329. *See generally Moalin*, 973 F.3d at 989.

330. *See generally id.*

331. *Id.* at 990.

332. *Id.* at 991.

amount of information collected by the NSA was extensive,[333] and it was essentially akin to twenty-four hour surveillance.[334] Furthermore, an extremely large amount of people had their telephony data collected by the NSA, enabling it to be aggregated and analyzed in bulk.[335] The argument that PRISM was a Fourth Amendment violation therefore had considerable force.[336] Government surveillance programs and how they fit into Fourth Amendment protections are thus starting to be questioned by the courts.[337]

Second, wrongful government surveillance could violate First Amendment rights to freedom of religion, speech, and association in some cases in which the government selectively targets individuals that speak, associate with, or belong to a certain religion.[338] Demonstrative of a First Amendment claim is *Fazaga*, in which the government targeted the plaintiffs for surveillance because they practiced Islam and associated with a local mosque.[339] Under Operation Flex, an FBI informant recorded conversations that took place in mosques, and the plaintiffs were surveilled solely because they were Muslims.[340] Yet *Fazaga* is just an example of the many instances of discriminatory targeted surveillance of Muslims since 9/11.[341] Currently, the government frequently uses discriminatory profiling for national security: mapping minority American communities around the country based on stereotypes about which groups typically commit certain crimes; scrutinizing Muslims at airports; and encouraging law enforcement agents and citizens to report "suspicious activity," a very vague standard that often results in surveillance of Muslims.[342]

---

333. *Id.*

334. *Id.*

335. *Id.* at 992.

336. *Id.*

337. *See generally id.* at 987.

338. *See, e.g.*, Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1213 (9th Cir. 2019).

339. *See generally id.* at 1212.

340. *See generally id.*

341. *See generally* Alexander J. O'Connor & Farhana Jahan, *Under Surveillance and Overwrought: American Muslims' Emotional and Behavioral Responses to Government Surveillance*, 8 J. MUSLIM MENTAL HEALTH 95, 96 (2014) (stating that government surveillance and post-9/11 discrimination caused American Muslims to experience "psychological distress"); *See also* Kelsey Dallas, *How 9/11 changed the government's relationship to American Muslims*, DESERET NEWS (Sept. 10, 2019, 10:00 PM), https://www.deseret.com/indepth/2019/9/10/20857801/9-11-american-muslims-government-surveillance [https://perma.cc/G8TP-ZVDR].

342. ACLU, *Anti-Muslim Discrimination*, https://www.aclu.org/issues/national-security/discriminatory-profiling/anti-muslim-discrimination [https://perma.cc/B5ZV-CRJ2] (last visited Aug. 2, 2021).

Wrongful government surveillance could further violate First Amendment rights to free speech by intercepting communications, chilling speech and ultimately preventing speech from occurring altogether.[343] When people know they are being watched or recorded, they are less likely to communicate frankly.[344] Although the court in *ACLU v. NSA* did not reach the merits of a First Amendment free speech violation due to a lack of standing, the court indicated that if it were certain that the NSA would intercept the plaintiffs' communications, and both parties to the communication were thus no longer willing to communicate with one another in the same way, a First Amendment claim for free speech could be established.[345]

Third, there could be a potential Fifth Amendment violation implicated by illegal government surveillance, denying plaintiffs equal protection of the law just because of their race or ethnicity.[346] *Fazaga* is again demonstrative, since the plaintiffs were singled-out and discriminated against solely for being of Middle Eastern descent.[347] In such a case, the government is essentially drawing a distinction between who they should target based on the person's race or ethnicity.[348] Equal protection thus requires that the governmental action be narrowly tailored to further a compelling government interest by the least restrictive means, a test that is very difficult to meet when the governmental action is facially discriminatory.[349] Targeting people of Middle Eastern descent just because of their race and ethnicity is likely a facially discriminatory governmental action, and should therefore be held unconstitutional.[350]

Yet the issue extends beyond the content of the plaintiff's case itself. The actual inability for a plaintiff to litigate his or her case also

---

343. *See generally Fazaga*, 916 F.3d at 1213; *see generally* Smith v. Maryland, 442 U.S. 735, 746–48 (1979) (Stewart, J., dissenting).

344. *See* United States v. White, 401 U.S. 745, 762–63 (1971) (Douglas, J., dissenting).

345. *See* Am. C.L. Union v. Nat'l Sec. Agency, 493 F.3d 644, 662 (6th Cir. 2007) (stating that "even if it were certain that the NSA would intercept these particular plaintiffs' overseas communications, if the overseas contacts were nonetheless willing to communicate with the plaintiffs by telephone or email in spite of the impending interception, then it is doubtful that the plaintiffs (journalists, academics, lawyers, or organizations), who have themselves alleged no personal fear of our government (or basis for fear of our government), would still be unwilling or unable to communicate.").

346. *See, e.g.*, *Fazaga*, 916 F.3d at 1213.

347. *See generally id.* at 1212.

348. *See generally id.*

349. *See* Strauder v. West Virginia, 100 U.S. 303, 307–09 (1879) (holding that it is unconstitutional to require that only white people can serve on juries); *see also* Loving v. Virginia, 388 U.S. 1, 11–12 (1967) (holding that it is unconstitutional to prevent an interracial marriage from occurring).

350. *See generally Fazaga*, 916 F.3d at 1213.

presents constitutional concerns. The first problem is that continued adherence by the judiciary to challenging procedural obstacles, like the state secrets privilege, undermines the constitutional system of checks and balances.[351] Currently, the state secrets privilege is functioning as almost an absolute and unchecked privilege for the executive branch, to shield the government and its agents from accountability for systemic violations of the Constitution.[352] An opportunity to bring a case against the government and obtain injunctive relief and damages for illegal surveillance is important because otherwise the government can act unchecked and without repercussions, infringing on individual rights without accountability.[353] The courts' continued acceptance of the state secrets privilege without scrutiny reduces the public's trust in the judiciary and thus weakens the constitutional system of checks and balances in the United States.[354]

The second problem arises under the Fifth Amendment Due Process Clause, affording plaintiffs the right to not be deprived of life, liberty, or property without due process of law.[355] As the law currently stands, the state secrets privilege is insulating government surveillance programs from judicial scrutiny, undermining the due process rights of individuals harmed by the programs.[356] Instead of being afforded the opportunity to be heard, plaintiffs are having their cases dismissed for lack of standing before they have a chance to build their case.[357] In cases where the government is the plaintiff suing a corporation or individual, judicial acceptance of the state secrets privilege should be even more reluctant.[358] In a regular criminal case, if federal prosecutors want to charge someone with a crime, the defendant has a right to documents to establish innocence.[359] Likewise, courts should not allow the suppression of government documents based on the states secrets privilege, when those documents could exculpate a defendant being sued by the government.[360] Otherwise the defendant is stripped of his or her right to a fair trial and to due process of the law.[361] For example, in *Gen. Dynamics Corp. v. United States* the

351. Herman, *supra* note 14, at 81.

352. ACLU, *supra* note 319.

353. *See generally id.*

354. THE CONSTITUTION PROJECT, REFORMING THE STATE SECRETS PRIVILEGE: STATEMENT OF THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE & COALITION TO DEFEND CHECKS AND BALANCES ii (2007); *see also* ACLU, *supra* note 319.

355. U.S. CONST. amend. XIV, § 1.

356. *See generally* THE CONSTITUTION PROJECT, *supra* note 354, at ii.

357. *See, e.g.*, Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *48–49 (N.D. Cal. Apr. 25, 2019); *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

358. *See generally* THE CONSTITUTION PROJECT, *supra* note 354, at 12.

359. *See generally id.*

360. *See generally id.*

361. *See generally id.*

court upheld a government claim of state secrets privilege precluding a government contractor's affirmative defense claim to government allegations of breach of contract.[362] Although not an electronic surveillance case, *Gen. Dynamics Corp.* demonstrates the lack of opportunity to defend against liability, as well as prove liability, when the government claims state secrets privilege.[363]

Another non-surveillance case that demonstrates the dramatic impact of the state secrets privilege on due process rights is *Kareem v. Haspel*, in which the plaintiff alleged he was on a United States "kill list" after being a near victim of at least five aerial bombings in Syria.[364] The government claimed state secrets privilege on the question of whether Kareem was being targeted for lethal action.[365] In granting the privilege, the judge noted that no constitutional right is more essential than the right to due process before the government may take a life, but that federal courts have limited authority to delve into the realms of national security concerns.[366]

B. Policy Problems

Even where government surveillance and the lack of judicial scrutiny in electronic surveillance cases does not violate a constitutional right, there are two prominent policy problems implicated by the state secrets privilege as it currently functions. First, current government surveillance of individuals and the third-party doctrine are chipping-away at individual privacy rights in the digital age.[367] Second, the denial of access to information critical for a plaintiff to establish standing undermines basic principles of justice in America because it enables the government to break the law without repercussions.[368]

First, current government surveillance and the third-party doctrine are jeopardizing individual privacy in the modern era.[369] The idea that one has a right to privacy is deeply rooted in American values.[370] As early as 1890, over a century before the right to privacy was recognized as a fundamental right stemming from the constitution,[371] legal scholars began recognizing that privacy protections must be continuously updated and

362. Gen. Dynamics Corp. v. United States, 563 U.S. 478, 486 (2011).
363. *See generally id.*
364. Kareem v. Haspel, 412 F. Supp. 3d 52, 55 (D.D.C. 2019).
365. *Id.* at 57–58.
366. *Id.* at 55, 61.
367. *See generally* Richards, *supra* note 222.
368. *See generally* THE CONSTITUTION PROJECT, *supra* note 354, at 12.
369. *See generally* Richards, *supra* note 222.
370. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).
371. *See* Lawrence v. Texas, 539 U.S. 558, 564 (2003).

extended to meet shifts in society and the economy.[372] Yet regulation and legislation lag behind technological developments, with technology-related bills still progressing through various stages in Congress, while new applications, devices, and software are being developed every day.[373] With society becoming increasingly dependent on technology in the workplace and private life, choosing between privacy rights or being connected is no longer a feasible option.[374] In fact, a 2018 study demonstrates that around fifty-four percent of Americans believe that companies do not have their best interests at heart, but are still willing to give up personal information if they see a benefit.[375] However, the third-party doctrine indicates that such personal information is not just stored and seen by the respective private company, but is also subject to being requested and used by the government.[376] Thus, devices like Google Home and Alexa that are now commonly used within the home and are collecting and storing voice recordings that take place in the privacy of one's home, are accessible by the government.[377] Consumers are potentially voluntarily giving away their personal data to the government and giving up their individual privacy rights without even knowing it.[378]

Second, the denial of access to information critical for a plaintiff to establish standing undermines principles of justice in America because it enables the government to commit statutory and constitutional violations without any consequence or remedy for the victim involved.[379] This result follows because under current precedent, the government can be almost certain that a plaintiff's case will be dismissed for lack of standing unless the plaintiff has obtained information to prove his or her particularized

372. Warren & Brandeis, *supra* note 370.

373. *Regulation and Legislation Lag Behind Constantly Evolving Technology*, BLOOMBERG L. (Sept. 27, 2019), https://pro.bloomberglaw.com/brief/regulation-and-legislation-lag-behind-technology [https://perma.cc/W9AC-ZCZN].

374. *See generally* United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

375. Robert Kurzer, *Gen Z, Millennials more willing to give up personal data in exchange for personalized experiences*, MARTECH (Sept. 11, 2018, 12:54 PM), https://martech.org/report-gen-z-millennials-more-willing-to-give-up-personal-data-in-exchange-for-personalized-experiences [https://perma.cc/6JGQ-XTY6].

376. *See* Ormerod & Trautman, *supra* note 223, at 110–11.

377. *See* Dorian Lynskey, *"Alexa, are you invading my privacy?"- the dark side of our voice assistants*, THE GUARDIAN (Oct. 9, 2019, 1:00 PM), https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants [https://perma.cc/88N6-5AEG].

378. *See generally* Kurzer, *supra* note 375; *see also* Ormerod & Trautman, *supra* note 223.

379. *See generally* THE CONSTITUTION PROJECT, *supra* note 354, at ii.

injury at the outset of the case.[380] Consequently, instead of courts achieving justice for the plaintiff, the plaintiff has nowhere to go to receive injunctive relief or damages for harms committed against him or her.[381]

VI. PROPOSED MODEL LEGISLATION

The following proposed model statute offers a solution to the government utilizing the state secrets privilege as a basis for thwarting the plaintiff's standing in alleged wrongful surveillance cases. This proposed statute explicitly curtails the government's ability to utilize the state secrets privilege in such a manner, while still protecting national security, by allowing the courts to compel withheld evidence from the government, conduct an *ex parte* and *in camera* review of that evidence, determine if the plaintiff has been wrongfully surveilled, and then move forward with the case by shielding unnecessary portions of the evidence to protect national security.

Standing for Electronic Surveillance Cases

I. Definitions:

1) "Electronic surveillance" means:[382]

> (A) The acquisition by an electronic, mechanical, or other surveillance device, of the contents or any wire or radio communication sent by or intended to be received by a particular United States person who is located in the United States, if the contents are acquired by intentionally targeting that United States person, and that person has a reasonable expectation of privacy and a warrant would usually be required;
>
> (2) The acquisition by an electronic, mechanical, or other surveillance device, of the contents of any wire communication to or from a person in the United States without their

380. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *48–49 (Cal. D. Ct. 2019); *see also* El-Masri v. United States, 479 F.3d 296, 313 (4th Cir. 2007).

381. *See generally* THE CONSTITUTION PROJECT, *supra* note 354, at ii.

382. This definition is based on FISA's definition of electronic surveillance. *See* 50 U.S.C. § 1801(f).

> consent, if the acquisition occurs in the United States, and does not include acquisition of communications of computer trespassers that is permissible under Section 2511(2)(i) of title 18 of the U.S.C.;
>
> (3) The intentional acquisition by an electronic, mechanical, or other surveillance device, of the contents of any radio communication sent and intended to be received in the United States, in which a person has a reasonable expectation of privacy and a warrant would usually be required; or
>
> (4) 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, in which a person has a reasonable expectation of privacy and a warrant would usually be required.

2) "Wrongfully surveilled" means the illegal use of surveillance against an individual, without a warrant, court order, or due cause, such as collateral surveillance.

3) "*Ex parte* and *in camera* review" is a review of one aspect of the case, such as standing, conducted by the judge in private, with only one party present, often the party claiming privilege on the material in question.

4) "Shield" as it pertains to shielding privileged governmental evidence includes methods such as bifurcating the evidence to only include evidence in the record needed for the plaintiff to prove an injury-in-fact; taking out entire pages of evidence from the record that will not be necessary for the plaintiff to make his or her prima facie case; blacking-out sensitive information with a permanent marker or equivalent technological tools, ensuring that the

blacked-out portions are unreadable; or sealing the evidence.

II. Standing in electronic surveillance cases:

In cases alleging wrongful electronic surveillance by the government, a plaintiff shall be afforded basis for suit that provides for damages and injunctive relief against the government.

A plaintiff shall be afforded standing under the following circumstances:

1) **Threshold Showing.** The plaintiff must make a threshold showing that he or she has been wrongfully surveilled by the government. A threshold showing means that the plaintiff must have reason to believe that he or she has been wrongfully surveilled. "Reason to believe" requires a cause beyond a mere hunch, instead rising to the level of reasonable suspicion. The court has discretion to determine if the plaintiff's threshold showing has been met.

2) **Compulsion.** Once the court has determined that the plaintiff has made a threshold showing, upon a claim of privilege by the government, the court must, *sua sponte* or on request of the plaintiff, compel the government to produce to the judge allegedly privileged evidence pertaining to the plaintiff's alleged injury.

3) ***In Camera* and *Ex Parte* Review.** The court must then conduct an *in camera* and *ex parte* review of the allegedly privileged information and determine whether the plaintiff was unlawfully surveilled. When conducting this review, the court must not consider edited documents or classified affidavits, declarations, or statements prepared as substitutes for the disputed evidence.

4) **Shielding of Evidence.** If the court determines that the plaintiff was wrongfully surveilled, the court must shield the allegedly privileged government evidence from national security concerns by only disclosing materials to the plaintiff relating to the surveillance that are necessary to make an accurate determination of the legality of the surveillance.

5) **Discretion.** The court has discretion in deciding how to shield allegedly privileged materials, and if the court determines that the material cannot be shielded from national security concerns, the court may dismiss the case. However, the court must make a substantial effort to shield the evidence and allow the case to go forward.

III. Authorization to lessen judicial burden:

1) **Appointment of FISA Judge.** In the interests of efficiency, the court may appoint a FISA judge to decide cases of electronic surveillance.

2) **Appointment of Special Masters.** The FISA judge or judge overseeing the case may further appoint Special Masters to:

(A) Make an initial determination of whether the plaintiff has met his or her threshold showing and file a report with the FISA judge or judge overseeing the case accordingly;

(B) Conduct the *in camera* and *ex parte* review of the allegedly privileged information; and

(C) Determine if the plaintiff has been wrongfully surveilled and thus has standing, and file a report with the FISA judge or judge overseeing the case accordingly for the FISA judge or judge overseeing the case to make the final determination.

> If a Special Master is appointed to the case, he or she must be qualified to work on electronic surveillance cases involving sensitive issues of national security. For example, he or she must receive an appropriate background check and be familiar with FISA procedures.

VII. REASONING FOR PROPOSED MODEL LEGISLATION

The above proposed model legislation offers a balanced solution to mend the constitutional and policy problems currently caused by the state secrets privilege by affording plaintiffs a basis for suit against the government when they have been wrongfully surveilled.

First, it is important to note that the overarching reason why this legislation focuses on standing, as opposed to reforming the common law state secrets privilege in its entirety, is practicality and efficiency. As explained in Section III, a plaintiff who has standing is also "aggrieved" under FISA. This means that if a plaintiff obtains standing in an electronic surveillance case, FISA procedures should apply to the remainder of the case. As a result, cases should no longer be dismissed under the common law *Reynolds* state secrets privilege once the plaintiff has obtained standing, but should instead proceed under FISA's more protective procedures. Therefore, reforming the state secrets privilege in its entirety would likely afford similar protections that FISA already provides once the plaintiff obtains standing. Yet entire reform of the state secrets privilege would be much more difficult to accomplish than heightened standing procedures, with the government presumably heavily opposed to its reform due to the national security risks involved with such reform.

Second, the above legislation directly addresses constitutional and policy problems created by the state secrets privilege by strengthening the constitutional system of checks and balances, restoring Fifth Amendment due process rights, and strengthening principles of justice. It primarily does this by requiring that the court compel and then review *in camera* and *ex parte* the actual allegedly privileged evidence to determine if the plaintiff has been wrongfully surveilled.

Mandating an *ex parte* and *in camera* review and a subsequent determination of whether the plaintiff was wrongfully surveilled is important because current precedent demonstrates that courts are not applying FISA procedures unless the plaintiff qualifies as "aggrieved."[383] Since the government is currently claiming privilege at such an early stage of litigation, on the mere question of whether the plaintiff is "aggrieved" or has standing, plaintiffs have no opportunity for FISA procedures to apply to their case, and thus no mandated judicial review of allegedly privileged

383. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *40.

evidence and a determination of whether the plaintiff was wrongfully surveilled.[384] Consequently, cases are being dismissed without judges reviewing the evidence,[385] which means plaintiffs are not receiving due process of the law, but are instead stripped of an opportunity to seek justice for their injury. Yet the entire reason for establishing judicial review was so that the courts can check the other branches of government by providing oversight and intervening when necessary.[386] Without judicial oversight, the government is able to commit constitutional violations and act inconsistent with the morals of society without reprimand, which is not justice, but governmental immunity.[387]

Even where courts *are* conducting an *in camera* and *ex parte* review of the evidence when FISA procedures do not apply, *Jewel* indicates that courts may review the evidence but will not then determine whether the plaintiff has been wrongfully surveilled, instead dismissing the case for lack of standing.[388] Conducting the review without determining if the plaintiff was wrongfully surveilled is problematic because it is essentially a pointless endeavor. Not only does it indicate that the courts are confused, applying half of FISA's procedures when the plaintiff has not yet shown he or she is aggrieved, but it also places an unnecessary burden on the judiciary, spending time and effort in conducting a review but not actually looking at the substance of the government's evidence when doing so. It is thus more efficient and effective for the courts to conduct the review *in order to* determine whether the plaintiff has been wrongfully surveilled, which is exactly what this proposed model legislation requires.

To ensure the plaintiff is receiving due process and to restore checks and balances, the court must review the actual, classified evidence when conducting the *in camera* and *ex parte* review, instead of any substitutes created by the government, so that the court can make a full and accurate determination of whether the plaintiff was wrongfully surveilled. Currently, judges will accept substitutes from the government for their allegedly privileged evidence, in the form of affidavits, declarations, or statements.[389] This means that the government is permitted to edit their evidence before it is reviewed by a judge.[390] Such authority makes judicial review ineffective, allowing the executive branch, an interested party, to shield its own evidence from scrutiny before the judge begins independent review.[391] Permitting the executive branch to perform a function of the judiciary not only upsets checks and balances, but also strips the adversarial

384. *See generally id.* at *48–49.
385. *See generally id.* at *49–50.
386. *See* Marbury v. Madison, 5 U.S. 137, 173–75 (1803).
387. *See generally id.*
388. *See Jewel*, 2019 U.S. Dist. LEXIS 217140, at *40.
389. *See generally* THE CONSTITUTION PROJECT, *supra* note 354, at ii.
390. *See generally id.*
391. *See generally id.*

party of their due process rights because the government could simply remove any details demonstrating injury to the plaintiff.[392] Moreover, allowing the government to use a substitute in any situation defies the Federal Rules of Evidence, which only allow a substitute to be provided when the original or duplicate is lost.[393] By requiring the government to produce the actual, raw evidence, the court is given full access to the facts and can make a complete determination as to whether the plaintiff has standing. Judges regularly review and evaluate highly classified information and documents,[394] so the same should be done for electronic surveillance cases.

Third, the above legislation further strengthens the constitutional system of checks and balances by striking a balance between the plaintiff's interest in his or her individual rights and the government's interest in national security. To protect the government's interest in national security, the court must conduct the review *ex parte*, in a private proceeding, to make sure that sensitive government evidence can be protected from the public eye to the greatest extent possible. Reviewing the evidence *ex parte* ensures that the content of the evidence is initially seen by no one but the judge and the government.[395] *Ex parte* hearings are commonly conducted by the judiciary when one party to the case claims privilege on certain discovery documents requested of them, and the court wishes to evaluate the privilege without violating the privilege itself.[396] Although there are arguable downsides to an *ex parte* hearing, courts have recognized that the competing objectives of the plaintiff and the government allow for some sacrifice of the adversarial process in cases implicating national security concerns.[397] In fact, an *ex parte* hearing has been recognized by the Ninth Circuit as an effective way, if not the only way, to protect the government's national security interests without stripping the plaintiff of his or her due process rights.[398]

If, following the *ex parte* and *in camera* review, the court determines that the plaintiff has standing to litigate his or her case, the court may use a variety of methods to ensure that the allegedly privileged

---

392. *See generally id.*

393. *See* Fed. R. Evid. 1002; *see also* Fed. R. Evid. 1003.

394. *The 'Orwellian' Bush administration*, WASH. TIMES (Oct. 29, 2007), https://www.washingtontimes.com/news/2007/oct/29/the-orwellian-bush-administration [https://perma.cc/V2VH-RH2Z].

395. Supplemental Brief for Donald Trump, et al. in Support of Defendants' Motion for Leave to Submit Documents *Ex Parte, In Camera* at 1–4, Wagafe v. Trump, 2018 U.S. Dist. LEXIS 76465 No. 2:17-cv-00094-RAJ (W.D. Wash. 2018).

396. *Id.* at 3.

397. *See* Am. C.L. Union v. Dep't of Def., No. 09-CV-8071, 2012 WL 13075286, at *2 (S.D.N.Y. Jan. 24, 2012).

398. *Id.*

evidence shows no more than necessary for the plaintiff to make his or her *prima facie* case. Judges are given considerable flexibility as to what methods they may use in order to maximize the plaintiff's opportunity of having his or her case move forward. However, the court is still given ultimate discretion to dismiss the case if there is absolutely no way to shield the government's evidence from sensitive issues of national security.[399] Providing judges with this discretion is necessary because it preserves a balance between the plaintiff's interests and national security interests.[400] In reality, not every case can be saved. A good example of such a case is *Totten*, wherein the entire judgement rested upon whether or not Lloyd worked as a secret agent and if so, how much compensation he was to be paid.[401] Clearly, the plaintiff could not recover unless it were proven that Lloyd worked as a secret agent, a fact that is in itself a secret.[402] If the court is not given discretion to dismiss a case such as *Totten*, the government's national security interests are at risk.

However, it is important to understand that discretion to dismiss the case should not be exercised unless as a *last resort*, and judges can by no means continue dismissing cases without making a significant effort to shield the evidence from national security concerns. This part of the model legislation is crucial because if courts do not make significant efforts to protect the evidence and move forward with the case, plaintiffs will end up in the exact same situation they are currently in. A good example of a case that should, theoretically, have been able to progress under this model legislation is *Jewel*. The case rested on whether a plaintiff's phone data was collected as a byproduct of the NSA's surveillance program[403] which, in itself, is not a national security issue like the situation in *Totten*. If the government in *Jewel* possessed records demonstrating that the plaintiffs' metadata were collected, a judge should have been able to black-out all information on those records besides the specific portion pertaining to the plaintiffs, without disclosing any top secret information that would jeopardize national security.

Finally, this legislation maintains a balance between the plaintiff's interests in his or her individual rights and the judiciary's interest in efficiency. First, to prevent a floodgate of litigation in response to the proposed model legislation and thus preserve judicial efficiency, the plaintiff is still required to make a threshold showing that he or she has been wrongfully surveilled before the court must act pursuant to this proposed legislation. A threshold showing requires a cause beyond mere

---

399. *See generally* Totten v. United States, 92 U.S. 105, 107 (1875).

400. *See* Fazaga v. Fed. Bureau of Investigation, 916 F.3d 1202, 1233-34 (9th Cir. 2019) (citing H. R. REP NO. 95-1283, pt. 1, at 21) (1978).

401. *See Totten*, 92 U.S. at 105–06.

402. *See id.* at 106.

403. *See* Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, 2019 U.S. Dist. LEXIS 217140, at *7–9 (N.D. Cal. Apr. 25, 2019).

suspicion, which is a very low burden on the plaintiff, designed not to serve as an obstacle, but merely to filter-out inadequate claims before the court expends resources and time pursuing the plaintiff's case. Without requiring that the plaintiff make a threshold showing, the courts could be bombarded with baseless claims brought by plaintiffs simply wishing to try their luck. Whereas requiring a threshold showing allows plaintiffs with genuine claims, such as those in *Jewel*, to finally receive their day in court.

"Reasonable suspicion" is the best standard to apply to the threshold showing because most plaintiffs with genuine claims are often able to obtain enough evidence to demonstrate more than a mere hunch that they were surveilled. For example, in *Jewel*, the plaintiffs had declarations of former AT&T technicians and a former AT&T employee indicating that they had likely been surveilled,[404] as well as proof that the NSA were collecting data at that time and that there was a non-compliance incident.[405] Cumulatively, this evidence shows that the plaintiffs, as AT&T customers, were likely included in the NSA's data collection program. Therefore, the plaintiffs in *Jewel* would have satisfied the threshold showing required in this model legislation.

Second, the court may assign a FISA judge to the case, and the FISA judge may further appoint qualified Special Masters to make certain recommendations. This is important for two reasons. First, the information reviewed includes sensitive national security information that FISA judges have experience reviewing and keeping confidential. Second, appointing FISA judges and Special Masters lowers judicial burden since the proposed model legislation requires judges to review a potentially large amount of evidence before even knowing whether the plaintiff has actually been wrongfully surveilled and has a valid claim. Allowing the court to appoint a FISA judge to the case with specialized knowledge on electronic surveillance lessens the resources required to determine whether the plaintiff has been wrongfully surveilled, decreasing the likelihood that the case will be overruled and reducing the time and resources needed to make an accurate determination. Furthermore, allowing the court to appoint qualified Special Masters to make important determinations in the case and file a report with the FISA judge or other overseeing judge also diminishes judicial burdens. This outsources the work that needs to be completed on the case, allowing Special Masters to conduct hearings, summarize, and make recommendations to the judge overseeing the case so that the judge can conclude the case more promptly.

404. *Id.* at *28–31.
405. *Id.* at *33–34.

CONCLUSION

The constitutional concerns and policy problems resulting from current government surveillance and the state secrets privilege indicate that the legislature needs to take action. It is axiomatic that the state secrets privilege is not a novel problem. Government surveillance abuses have been consistently debated in Congress and reformation attempts have been made. Yet currently, courts are still applying the 1953 "reasonable danger" test from *Reynolds* when FISA does not apply, thus dismissing cases without reaching the merits of the plaintiff's claims, even though technology has moved well-beyond what existed when *Reynolds* was decided. If nothing is done to clearly and precisely textualize the state secrets privilege, it will continue to be inconsistently applied by the circuit courts and the government will continue potentially violating individual rights without any repercussions. With the advancement of technology and society's increasing dependence on it, the state secrets privilege needs to be reformed now more than ever before to preserve individual rights from continued abuse by the government.

The solution begins with the legislature. The proposed model legislation in this Note contains key provisions that should be included in legislation passed by Congress for plaintiffs to achieve standing in a case where the government claims state secrets privilege. Although the proposed model legislation does not address every issue created by the state secrets privilege, it will provide an easier avenue for plaintiffs to achieve standing and a mechanism for judges to provide more judicial oversight for cases of alleged illegal government surveillance. By requiring judges to involve themselves more in helping plaintiffs achieve standing, plaintiffs will be able to bypass preliminary stages of their case and have a fighting chance to prove that they were illegally surveilled by the government.