PAY NO ATTENTION TO THE MAN BEHIND THE CURTAIN: THE GOVERNMENT'S INCREASED USE OF THE STATE SECRETS PRIVILEGE TO CONCEAL WRONGDOING

By Margaret Ziegler

I. INTRODUCTION

In the last forty years, the courts and legislature have taken steps to rein in the government's ability to wiretap U.S citizens, mostly in response to revelations of widespread government abuse of the practice. Most statutes and case law pertaining to wiretapping originated in the late 1960s and the 1970s.[1] Around this time, American mistrust of the government had increased greatly in the face of publicity surrounding the Watergate investigation, which uncovered massive unchecked government wiretapping of U.S. citizens.[2] Congress responded by codifying warrant obligations for electronic surveillance.[3] During and following the Vietnam War, litigation tested the government's right to eschew these requirements when faced with national security concerns. The Supreme Court addressed the issue in 1972, holding the warrant requirement for eavesdropping on U.S. citizens is mandated by both statute and the Fourth Amendment.[4]

Following the attacks of September 11, 2001, the United States became involved in another literal war as well as a figurative war on terrorism. The government once again began eavesdropping on its citizens and using national security as its justification.[5] With many eavesdropping practices outlawed in the 1970s, the government has now taken steps to conceal its surveillance activities. When questionable activities are uncov-

---

1. *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510-21 (2000) [hereinafter "The Wiretap Act"]; Foreign Intelligence Surveillance Act, Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811) (2000) (these sections pertain to electronic surveillance) [hereinafter "FISA"].

2. *See generally* Barbara B. Altera & Richard S. Pakola, *Master Environmental Edition II: All the Information the Security of the Nation Permits*, 58 A.F. L. REV. 1, 7 (2006) (describing "a post-Watergate general increase in distrust of government").

3. *See* The Wiretap Act and FISA, *supra* note 1.

4. *See* United States v. United States Dist. Court, 407 U.S. 297 (1972) [hereinafter "*Keith*"].

5. *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006); ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007).

ered and lawsuits are filed, the government has a unique shield to hide behind. A little-known common law evidentiary privilege, the state secrets doctrine, allows the government to withhold allegedly secret evidence from courts and to block unwanted lawsuits.[6]

When secret government activities might be uncovered by a lawsuit, the state secrets privilege allows the government to block the release of any information or documents that might harm national security.[7] In theory, this is an important tool to ensure that the broad discovery allowed in most lawsuits does not allow government secrets to fall into the wrong hands. "Say, for instance, that a janitor in Los Alamos, N.M., tripped over a box of uranium lying in the hallway in 1943. It would hardly do to have the evidence used in the subsequent slip-and-fall case scuttle the entire Manhattan Project."[8]

Today, however, even more so than in the 1970s, there is a real danger that the government is using the privilege not to protect national security, but to cover up its own wrongdoing.[9] During the Bush administration, not only has use of the state secrets privilege increased greatly, but the privilege has also expanded from a narrow evidentiary privilege to a full-blown litigation killer.[10]

This Note focuses on the government's use of the state secrets privilege to avoid judicial review of its wiretapping activities, and examines the expansion of the privilege—especially its developing use as a screen between government wrongdoing and judicial scrutiny.

Part II discusses the holding in *Hepting v. AT&T*, a recent lawsuit challenging widespread government wiretapping of American citizens and the district court's refusal to dismiss the case on state secrets grounds. Part III traces wiretapping's technological developments and the progression of laws intended to regulate the government's use of this technology against American citizens. Part III also examines the origin of the state secrets doctrine, which predated all of these developments. Part IV turns to government attempts to use the state secrets privilege to avoid the courts' and legislature's attempts at regulating wiretapping and argues that wiretapping exemplifies the state secrets privilege's misapplication to cover up government wrongdoing. Part V advocates for a reversal of the privilege's

---

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

7. *Id.*

8. Henry Lanman, *Guarding Secrets*, SLATE, May 22, 2006, http://www.slate.com/id/2142155/ (last visited Apr. 5, 2008).

9. *See* Part V *infra*.

10. *See* Part IV *infra*.

evolution from a narrow evidentiary rule to a tool of government immunity.

II. *HEPTING V. AT&T*: CLAIMS AND PROCEEDINGS SO FAR

In 2005, after twenty-two years at AT&T, retired technician Mark Klein paid a visit to the Electronic Frontier Foundation (EFF), an advocacy group, and handed over documents that he claimed blew the whistle on secret National Security Agency (NSA) wiretapping activities.[11] He contends that AT&T had assisted the government in large-scale spying on American communications.[12] If Klein's allegations are correct, AT&T has granted the government unfettered access to all of its customers' communications, permitting the NSA to spy on virtually any U.S. citizen without a warrant.[13]

In response to the documents produced by Klein, the EFF filed a class action lawsuit on behalf of AT&T's customers.[14] In the resulting suit, *Hepting v. AT&T*, plaintiffs allege that AT&T's wiretapping activities occur under color of law and violate both Constitutional and statutory requirements, including the Foreign Intelligence Surveillance Act (FISA).[15] The plaintiffs also allege that, under FISA, telecommunication companies have an independent duty to their customers to protect the contents of their communications unless the government obtains a warrant.[16]

The government responded to the *Hepting* lawsuit by intervening as a co-defendant and asserting, among other defenses, the state secrets privilege.[17] The Northern District of California rejected the government's motion to dismiss under the state secrets privilege, saying, "[t]he government has opened the door for judicial inquiry by publicly confirming and denying material information about its monitoring of communications content."[18] The case was immediately appealed to the Ninth Circuit and

---

11. For Mark Klein's account, see *Wiretap Whistleblower's Account*, WIRED, April 7, 2006, http://www.wired.com/science/discoveries/news/2006/04/70621.

12. *Id.*

13. *Id.*

14. *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006).

15. *See id.* at 978.

16. E-mail interview with Cindy Cohn, EFF Counsel in *Hepting* (Nov. 29, 2007 and Jan. 1, 2008) [hereinafter "Cohn Interview"].

17. *See Hepting*, 439 F. Supp. 2d at 979.

18. *Id.* at 996.

though the parties presented arguments on August 15, 2007, an opinion has not yet been issued at the time this Note went to press.[19]

The central allegation in *Hepting* is that AT&T and the government, in violation of FISA and the Wiretap Act, have set up a surveillance system which essentially acts as a "dragnet" that collects the content of *all* customers' Internet and phone communications that travel through AT&T's fiber optic wires.[20] Klein claims that AT&T has not only consented to the government breaching its fiber optic wires, but has allowed a secret room to be built at its Folsom Street location in San Francisco, where a portion of the light from the wires is diverted to high-tech surveillance equipment which analyzes the data and transmits part or all of it to the government.[21] While the most direct evidence provided by Klein focuses on Internet communications (e-mail, web traffic, data, etc.), the *Hepting* plaintiffs allege that AT&T has allowed the NSA access to telephone communications traveling through its networks as well.[22]

The government, as an intervening defendant, moved to dismiss or, alternatively, for summary judgment based mainly on the state secrets privilege.[23] Judge Walker of the Northern District of California refused to dismiss the case or grant summary judgment for plaintiffs' claims against AT&T or the government for allegedly collaborating to form a massive warrantless wiretapping operation.[24] The court noted that, following September 11, President Bush admitted to authorizing the NSA to perform surveillance of telephone communications where one party is located outside the United States and the government has a reasonable basis to conclude that one party has connections with or supports the al Qaeda terrorist group.[25] The court also took note of Klein's allegations that, while working at an AT&T office in San Francisco, he saw a room being built which contained "technology . . . known to be used particularly by government intelligence agencies"[26] and learned of documents describing how equip-

19. Unofficial Transcript of Oral Argument, Hepting v. AT&T, No. 06-17132 (9th Cir. Aug. 15, 2007), http://www.eff.org/files/filenode/att/hepting_9th_circuit_hearing_transcript_08152007.pdf (last visited Apr. 5, 2008).

20. *See Hepting*, 439 F. Supp. 2d at 1001.

21. *Id.* at 989.

22. *See* Cohn Interview, *supra* note 16.

23. *See Hepting*, 439 F. Supp. at 979. AT&T also moved to dismiss, contending that plaintiffs lacked standing and did not affirmatively plead that AT&T's actions were not certified by the government. They also asserted statutory theories, common law immunity, and qualified immunity. *Id.* at 999. The court denied all of these. *Id.* at 1001-1010.

24. *Id.* at 1011.

25. *Id.* at 986-987.

26. *Id.* at 989.

ment tapped into AT&T's circuits and diverted "some of the light signal to the secret room."[27]

The district court opinion identified from precedent the three ways the state secret privilege can require dismissal of a case.[28] First, if the "very subject matter of the action" is a state secret, the court must dismiss the action.[29] Second, the government can privilege specific evidence, leaving the plaintiff unable to prove the prima facie elements of his or her case.[30] Finally, if information classified as privileged prevents a defendant from raising an otherwise valid defense, summary judgment must be granted for the defendant.[31]

The government maintains that these three forms of the state secrets privilege are legitimate, and argues that all three apply in *Hepting*.[32] Regarding the first, the government claims that the very subject matter of the case is a state secret. Regarding the second approach, the government says the plaintiffs will not be able to establish the prima facie elements of their case because the state secrets privilege protects "any information tending to confirm or deny (a) the alleged intelligence activities, (b) whether AT&T was involved with any such activity and (c) whether a particular individual's communications were intercepted. . . ."[33] The government claims invoking the privilege precludes a "fact-intensive inquiry" without which Hepting cannot prove the searches unreasonable.[34] Finally, the government asserts the third version by arguing that state secrecy deprives AT&T of a potential defense—authorization by the government.[35]

With respect to the "very subject matter" argument, the district court concluded that the public knew enough (and the government had disclosed enough) about the surveillance programs to foreclose the possibility that the "very subject matter" of the action was a state secret.[36] Quoting President Bush's public addresses, newspaper articles, and AT&T's statements, the court found that this was "not the kind of 'secret' that . . . the state se-

27. *Id.*
28. *Id.* at 984.
29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.* at 985.
33. *Id.*
34. *See id.* at 985.
35. *Id.* at 986.
36. *See id.* at 994.

crets privilege [was] intended to protect or that a potential terrorist would fail to anticipate."[37] The court continued:

> AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content . . . the government has publicly admitted the existence of a 'terrorist surveillance program' . . . [which] operates without warrants . . . [and c]onsidering the ubiquity of AT&T telecommunications services, it is unclear whether this program could even exist without AT&T's acquiescence and cooperation.[38]

Having completed an in camera review of the classified documents,[39] which traveled by armed guard from Washington, D.C., Judge Walker found them insufficiently secret to dismiss the case.[40]

With respect to the second and third approaches to state secrets identified in the opinion, Judge Walker said it would be premature to conclude that state secrets privilege would bar evidence that would keep Hepting from establishing his prima facie case or preclude AT&T's defense.[41] The court said its decision to allow the case to proceed followed precedent in other state secret cases where the courts allowed them to "proceed to discovery sufficiently to asses the state secrets privilege in light of the facts."[42]

III. WIRETAPPING TECHNOLOGY, PRIVACY LAW, AND STATE SECRETS

Section III.A explains why government ability to wiretap increasingly requires the cooperation of telecommunications carriers. Section III.B traces the key court decisions and statutes that limit government wiretapping of American citizens. Section III.C traces the development of the state secrets doctrine, the invocation of which, if successfully invoked in *Hepting*, could thwart efforts to ascertain compliance with statutory and Constitutional limits on contemporary wiretapping.

---

37. *Id.* at 993.
38. *Id.* at 991-992.
39. *Id.* at 980.
40. See Nat Hentoff, An Expansive View of 'State Secrets'; Federal Judge Shows Courage in Challenging Bush; WASH. TIMES, Aug. 14, 2006, at A15.
41. *See Hepting*, 439 F. Supp. 2d at 994.
42. *Id.* at 994.

A. Technical Background on Wiretapping

FISA and the Wiretap Act, the two primary statutes Hepting accuses AT&T of violating, were passed to prevent telecommunication companies and the government from colluding to spy on Americans.[43] When Congress passed the Wiretap Act, it recognized the need to impose on telecommunication companies an independent duty to protect their customers' private communications.[44] FISA's passage followed discoveries by the Senate that, during the 1950s, Western Union and other communication companies had turned over to the NSA millions of telegrams sent or received by U.S. citizens.[45] However, because of the nature of satellite communications, for most of the time since Congress enacted FISA and the Wiretap Act, the government has not needed telecommunication companies to facilitate spying on Americans.

Until recently, the government could capture much worldwide communication data without the help of any third party.[46] Starting in the 1960s, telecommunications increasingly relied on satellites.[47] Telephone signals traveled along wires from handsets to antennas, then bounced off satellites in space back down to receptor stations on the ground. It was easy for the NSA to place its own receptor stations alongside those of telecommunication companies and obtain its own copy of the data when the signals bounced from the satellites back to earth. With a few strategically-placed ground stations, the government could listen in on almost any conversation on the planet.[48]

---

43. *See* The Wiretap Act, 18 U.S.C. § 2516 (2000) (establishing warrant requirements for electronic surveillance); *see also*, Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811, 814 (2007) ("[FISA] was born in the late 1970s out of widespread revulsion at abuses by the Executive Branch of its information gathering authorities—in particular, warrantless wiretapping of dissident groups and the political rivals of incumbent statesmen.").

44. *See* Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 259 (9th Cir. 1977) ("[The Wiretap Act] recognizes that the integrity of the communications system demands that the public be assured that employees who thus come to know the content of messages will in no way breach the trust which such knowledge imposes on them.").

45. *See* Susan Landau, *National Security on the Line*, 4 J. ON TELECOMM. & HIGH TECH. L. 409, 447 n.104 (2006) (describing how "tapes of all international telegrams from RCA Global, ITT World Communications, and Western Union International were shipped daily to the NSA").

46. *See* PATRICK RADDEN KEEFE, CHATTER 51-52 (2005) (offering a detailed explanation of government capabilities for satellite interceptions).

47. *See id.* at 52.

48. *See id.*

Fiber optic cables have recently supplanted satellites, making telecommunications more challenging to infiltrate.[49] Fiber optic cables carry pulses of light, rather than electricity, and the content of the communications does not bounce indiscriminately into the government's receivers.[50] In order to monitor the content traveling along a fiber optic wire, one must physically breach the cable and divert the light pulsing through the strands of glass within the cable.[51] The need for a physical breach in the fiber optic cables, such as those used in AT&T's Folsom Street location, requires access to the cables—making the cooperation of a telecommunications carrier desirable, perhaps even necessary.[52] Once the cable is breached and the light is successfully diverted, an exact copy of each customer's communication data can be created.[53]

B. Regulation of Government Wiretapping in the Face of National Security Concerns

The Supreme Court initially determined that the Fourth Amendment did not apply to wiretaps.[54] In *Olmtead v. United States*, a Prohibition-era bootlegger objected to evidence used against him in a criminal proceeding that was obtained through a warrantless wiretap.[55] The court found that "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment."[56] Because the wiretap collected intangible material, nothing was seized and because there was no "physical invasion" of his home, there was no search.[57] Therefore, no Fourth Amendment violation occurred through the use of a warrantless wiretap and the evidence was admissible.[58]

Justice Brandeis presciently wrote in his *Olmstead* dissent:

> [T]he progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways

---

49. *See id.* at 73-74 (detailing the difficulty of monitoring fiber optic cables compared to earlier technologies).

50. *Id.*

51. *See id.*

52. *See* Cohn Interview, *supra* note 16.

53. *Id.*

54. Olmtead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 398 U.S. 347 (1967) *and* Berger v. New York, 388 U.S. 41 (1967).

55. *Id.* at 456.

56. *Id.* at 466.

57. *Id.*

58. *See id.* at 469.

> may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[59]

The court in *Hepting* today is dealing with just such a case. Technology has created a way for the government to remove our papers from our drawers as copies of our e-mails can be pulled from AT&T's fiber optic cables and duplicated. Brandeis concluded that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[60]

The issue of national security did not arise in *Olmstead*, a bootlegging case. However, the government raised national security concerns in *Katz v. United States*, the case that overturned *Olmstead* forty years later.[61] There, the government procured evidence of plaintiff's illegal gambling by wiretapping a phone booth.[62] The Supreme Court held that warrantless electronic surveillance in a criminal investigation was per se unreasonable under the Fourth Amendment.[63] The Court reasoned:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[64]

Justice Harlan's concurrence created the standard of protecting those situations where a person has a "reasonable expectation of privacy."[65] The government asserted in its briefs the concern that national security might require warrantless wiretaps, but the *Katz* Court explicitly declined to decide whether a national security exception to Fourth Amendment warrant requirements might apply, stating that the facts of *Katz* did not require such analysis.[66]

---

59. *Id.* at 474.
60. *Id.* at 478-79.
61. Katz v. United States, 389 U.S. 347 (1967).
62. *Id.* at 348.
63. *Id.* at 357.
64. *Id.* at 351.
65. *Id.* at 360.
66. *Id.* at 359 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is

The following year, in response to *Katz*, the standard of requiring warrants for electronic surveillance was codified in the Wiretap Act of the Omnibus Crime Control and Safe Streets Act.[67] The Wiretap Act authorizes electronic surveillance, subject to court order.[68] The statute also addresses national security concerns, specifically noting:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack . . . [or] to obtain foreign intelligence information deemed essential to the security of the United States . . .[69]

This proviso was carefully inserted by the government to allow intelligence gathering to continue despite the legislature's intention to curtail invasions of privacy. Roy Banner, a lawyer at the NSA, secretly assisted with the drafting of that provision and considered it a loophole for NSA's operations.[70] He sent a memo to the director of the NSA on July 24, 1968, saying that the exception was not only to "remove any doubt as to the legality of SIGINT[71] . . . operations of the Executive Branch of the Government" but also that the language "precludes an interpretation that the prohibitions against wiretapping or electronic surveillance techniques in other laws applies to SIGINT . . . activities of the Federal Government."[72]

Five years later, in *United States v. United States District Court* (known as *Keith*), the Supreme Court had the opportunity to revisit the issue that they had passed on in *Katz* and discuss whether a national security exception to warrant requirements existed.[73] In *Keith*, a defendant was charged with a dynamite explosion at a CIA office and two others were changed with conspiring to destroy government property.[74] The defendants requested documentation of electronic surveillance that was obtained without a warrant prior to their arrest to determine if it "tainted" their indictment.[75] Beyond bootlegging in *Olmstead* and illegal gambling

---

a question not presented by this case."); *see also* Michael A. DiSabatino, *Construction and application of "national security" exception to Fourth Amendment search warrant requirement*, 39 A.L.R. FED. 646 (1978).

67. *See* 18 U.S.C. §§ 2510-2521 (2000).

68. *Id.*

69. *Id.* § 2511(2)(f).

70. *See* James Bamford, The Puzzle Palace 326 (1982).

71. SIGINT is short for "signals intelligence" or intelligence gathering by intercepting signals. *See* Church Report, *infra* note 84.

72. BAMFORD, *supra* note 70, at 326.

73. *See Keith*, 407 U.S. 297 (1972).

74. *Id.* at 299.

75. *Id.* at 300.

in *Katz*, this case had *actual* national security issues at stake. Nevertheless, the Court unanimously held that the government's surveillance actions were unlawful and that the national security implications did not justify departing from the warrant requirements in the Wiretap Act.[76] The *Keith* Court, however, urged Congress to create legislation to specifically deal with "the precise standards for domestic security warrants."[77] While *Keith* did not address the need for a warrant to perform the electronic surveillance on foreign powers or agents, it left no doubt that purely domestic surveillance without a warrant was forbidden by the Wiretap Act.[78]

Following the Supreme Court's holding in *Keith*, the legality of the NSA's MINARET program (which contained a watch list of both foreign and domestic persons whose communications were monitored and disseminated to law enforcement agencies) was called into question—especially because some people being monitored had no foreign ties.[79] Then Attorney General, Elliot Richardson, wrote a memo to the head of the NSA and, citing *Keith*, directed the NSA to "'curtail the further dissemination' of watch list information to the FBI and Secret Service, although 'relevant information acquired by you in the routine pursuit of the collection of foreign intelligence information may continue to be furnished.'"[80] Compared to the millions of customers allegedly being monitored in *Hepting*, Richardson was concerned with eavesdropping on just over 600 individuals on the MINARET watch list, only *some* of whom were Americans.[81] Following *Keith*, Attorney General Richardson felt it was too obviously illegal to allow such warrantless domestic surveillance to continue.[82]

Soon after *Keith*, the Senate-created Church Committee uncovered more questionable information-gathering practices,[83] including Operation

---

76. *See id.* at 324.

77. *Id.* at 323.

78. *Id.* at 323-324 ("We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.").

79. BAMFORD, *supra* note 70, at 372.

80. *Id.*

81. *Id.* at 371.

82. *See id.*

83. The *Keith* case overlapped with the Watergate scandal. As the government's investigation into Watergate and the Nixon administration progressed, massive-scale wiretapping of the American people was among the improprieties discovered that led to the Church Committee's appointment. *See* Susan Freiwald, *Online Surveillance*, 56 ALA. L. REV. 9, 12 (2004) (describing the revelations of illegal wiretapping during the Watergate investigations).

MINARET,[84] Operation SHAMROCK,[85] and a mission that the CIA's own General Counsel had determined violated the Wiretap Act.[86] Following embarrassing revelations—including the monitoring of Dr. Martin Luther King, Jr. and organizations participating in the women's liberation movement in the name of national security[87]—Congress answered the Church Committee recommendations[88] and the Supreme Court's call for guidance on foreign intelligence gathering by enacting FISA in 1978.[89]

FISA regulates the government use of warrantless surveillance on international parties when American citizens are also being wiretapped. The statute requires the executive branch's representatives to apply to the Foreign Intelligence Surveillance Court (FISC) for a warrant to conduct foreign intelligence surveillance anytime a "United States person" is likely to be one party to the communication being monitored.[90] The court must find probable cause that the other party being targeted is a foreign power or an agent of a foreign power and that the information sought is foreign intelligence information.[91] FISA also contains ambiguously worded "minimization requirements" to protect the U.S. citizen.[92] If FISA requirements are

84. S. Select Comm. to Study Governmental Operations With Respect To Intelligence Activities, Supplementary Detailed Staff Reports on Intelligence Activities And The Rights Of Americans, Book III, Final Report § 1(B) ¶ 1 (1976), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIj.htm (hereinafter "Church Report"): MINARET was described by the Church Report as a government-sponsored watch list including people whose communications were specifically monitored and disseminated to intelligence organizations. The list included "American groups and individuals whose activities 'may result in civil disturbances or otherwise subvert the national security of the U.S.'" *Id.* For Minaret charter reproduced in part see Bamford, *supra* note 70, at 323-24.

85. *Id.* § 1(B) ¶ 2 ("From August 1945 until May 1975, NSA received copies of millions of international telegrams sent to, from, or transiting the United States. Codenamed Operation SHAMROCK, this was the largest governmental interception program affecting Americans.").

86. *Id.*

87. Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 334 (2005).

88. *See* Freiwald, *supra* note 83; *see also*, Sales, *supra* note 43.

89. *See* FISA, 50 U.S.C. § 1805 (2000).

90. *See* FISA, 50 U.S.C. § 1804(b) (2000).

91. *See* FISA, 50 U.S.C. §§ 1804-05 (2000).

92. *See* FISA, 50 U.S.C. § 1801(h) (2000) (requiring the Attorney General to establish specific procedures "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons").

met, a judge must issue a warrant without discretion.[93] Additionally, in emergency situations where a warrant cannot be obtained immediately, the Attorney General can authorize up to seventy-two hours of surveillance and the order can be approved retroactively.[94]

The FISC has historically been shrouded in secrecy and very compliant with the government's warrant requests. From its windowless, soundproof, cipher-locked room on the top floor of the Justice Department, the court deals out FISA warrants liberally.[95] Since the court's inception, almost every single warrant requested has been granted.[96] The operation of FISC is unlike any other court in the United States. There are no adversarial proceedings; no witnesses are cross-examined; and only the government is permitted to present its side of the story.[97] The eleven rotating judges are selected by the Chief Justice of the Supreme Court in secret.[98] Almost no opinions are issued and all rulings are permanently sealed.[99] Since September 11, 2001, the court has approved about one thousand applications per year—more than three each day—and has only refused a handful.[100]

C. The Origin of the State Secrets Doctrine and its Expansion Towards Blanket Immunity

The state secrets doctrine received its first official treatment by the Supreme Court in *United States v. Reynolds*. When *Reynolds* was decided, wiretapping was not yet restricted under the Fourth Amendment or any

---

93. *See* FISA, 50 U.S.C. § 1805(c) (2000) ("[T]he judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds . . . [requirements are met].").

94. *See* FISA, 50 U.S.C. § 1805(f) (2000).

95. James Bamford, *Washington Bends the Rules*, N.Y. TIMES, Aug 27, 2002, at A2, *available at* http://query.nytimes.com/gst/fullpage.html?res=9B04EEDA113CF934A1575BC0A9649C8B63.

96. *See* KEEFE, *supra* note 46, at 159.

97. *See id.* at 158.

98. *Id.*

99. *Id.*

100. The Attorney General must report to Congress under FOIA the number of orders requested, granted and denied in a given year. This information is publicly available. In 2005, 2,072 applications were approved and none were denied in whole or in part. In 2004, FISC approved 1,754 applications and denied none. In 2003, the court approved 1,724 applications and denied four—two of which were reconsidered and approved in whole or in part shortly afterward. All 1,228 applications made in 2002 were approved. All 934 requests of 2001 were approved. Reports from 1996-2005 are available online. *See* DEPARTMENT OF JUSTICE, ANNUAL FOREIGN INTELLIGENCE SURVEILLANCE ACT REPORTS (2001-2005), *available at* http://www.usdoj.gov/ag/readingroom/ag_foia1.htm (last visited Apr. 5, 2008).

other law.[101] Because warrantless wiretapping was not yet recognized as unlawful and because technology was not nearly as advanced as it is today, it is difficult to imagine the *Reynolds* Court could have foreseen its application in covering up the massive government spying on American citizens that is now at issue in *Hepting*. The case was about military secrets in the context of a military mission. In 1953, an Air Force flight crashed in Georgia, killing, among others, three civilian engineers.[102] The decedents' widows sued, claiming negligence and, during discovery, sought production of the official accident report.[103] The government filed a formal "Claim of Privilege" which said that producing the information would have negative effects on national security.[104]

The Supreme Court harkened back to English law and U.S. cases as early as 1807 to find precedent to support a claim of state secrets.[105] Then, without examining the purported secret document, the Court accepted the government's assertion and established procedural requirements for asserting the privilege.[106] To employ the state secrets privilege the government's claim must be 1) formal, 2) "lodged by the head of the department which has control over the matter, and [3)] made after actual personal consideration by that officer."[107] A court deciding whether to apply the privilege is not required to examine the secret evidence, and, depending on the circumstances, may not be permitted to do so. Essentially, the *Reynolds* standard takes the government at its word that the evidence requested, if revealed, would be detrimental to national security.[108]

Fifty years after *Reynolds*, the daughter of one of the men killed, Judy Loether, accidentally learned on the Internet that the accident report had been declassified.[109] She purchased a copy from a private company for $63. "To her utter amazement, the accident report revealed that no state secrets whatsoever had been involved; rather, the only secret was the gross negligence by the military."[110] The report revealed negligent operation and

101. *See generally* United States v. Reynolds, 345 U.S. 1 (1953).
102. *Id.* at 3.
103. *Id.*
104. *Id.* at 4.
105. *Id.* at 7-8.
106. *Id.* at 11.
107. *Id.* at 7-8.
108. *Id.*
109. John W. Dean, ACLU v. National Security Agency: Why the "State Secrets Privilege" Shouldn't Stop the Lawsuit Challenging Warrantless Telephone Surveillance of Americans, FindLaw, June 16, 2006, http://writ.news.findlaw.com/dean/20060616.html (last visited Apr. 5, 2008).
110. *Id.*

pilot error as among the causes of the crash, and only mentioned the secret mission of the plane in passing.[111] Ms. Loether believes that the government actually invoked the state secret privilege to avoid embarrassment.[112] This would not be the only time the government would do so.[113] Thus, besides creating the state secrets privilege, *Reynolds* exemplifies the pressing need for judicial oversight of such executive claims of secrecy.

Questioning the government's assertion of the privilege is the exception and not the rule. Historically, when the state secrets doctrine has been invoked, courts have been reluctant to investigate the executive's claim of secrecy. In fact, courts have only rebuffed the government's use of the privilege on four occasions.[114] In *Halpern v. United States*, a patent suit involving an invention with military applications, the Second Circuit allowed the district court to hold the entire trial in camera if necessary to protect national security.[115] The Second Circuit held that "the privilege relating to state secrets is inapplicable when disclosure to court personnel in an in camera proceeding will not make the information public or endanger the national security."[116] In *Republic Steel*, the court found that two cables from the Department of Commerce to the American Embassy in Bucharest were not privileged following in camera review.[117] Rejecting an "entirely conclusory" allegation that the documents at issue posed a threat to national security the court found they were not shown to be "in the same class as those for which the state secrets privilege has been recognized."[118] Less than two years later, the same court rejected the Commerce

---

111. Matt Katz, *Air Force Report Undermines Secrecy Rationale*, COURIER POST ONLINE, June 24, 2005, http://www.courierpostonline.com/specialreports/statesecrets/m062403b.htm (last visited Apr. 5, 2008).

112. *See* Dean, *supra* note 109.

113. *See* United States v. New York Times, 403 U.S. 713 (1971). In this case, the federal government cited "grave and irreparable" danger to national security in an attempt to prevent national newspapers from publishing the Pentagon Papers. The Supreme Court allowed the release of the documents and "most observers agree that the publication of the papers did not do injury to the national security of the United States." *See The Pentagon Papers Case*, 2 EJOURNAL USA, February 1997, http://usinfo.state.gov/journals/itdhr/0297/ijde/goodsb1.htm (last visited Apr. 5, 2008). In fact, the Solicitor General responsible for the government's brief later admitted in an editorial, that "governmental embarrassment" and not national security was the principal concern. Erwin N. Griswold, *Secrets Not Worth Keeping*, WASH. POST, Feb. 15, 1989, at A25.

114. William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85, 100 (2005).

115. Halpern v. United States, 258 F.2d 36, 44 (2d Cir. 1958).

116. *Id.*

117. Republic Steel Corp. v. United States, 3 C.I.T. 117, 118 (1982).

118. *Id.*

Department's assertion of the privilege when in camera review showed the documents merely "consist[ed] of material regarding the financial condition of two Brazilian steel companies."[119] Finally, in *Yang v. Reno*, the court found that the formal threshold *Reynolds* requirements had not been met, but said the government would be "given the opportunity to re-assert the privilege[]."[120] Of these exceptions, only in *Halpern* did the court truly confront the need to try a case despite recognized national security worries; in *Republic Steel* and *United States Steel*, the information was obviously not a secret of the state; in *Yang*, use of the privilege was merely delayed by failure to meet *Reynolds* formalities. In the only two cases where the government's invocation was rejected because the information was not secret, the court realized this by examining the documents in camera.

A notable district court case, *Spock v. United States*, did not reject use of the privilege, but asserted limits, stating that "the states secrets privilege is only an evidentiary privilege, which should be construed narrowly, to permit the broadest possible discovery consistent with the purposes of the privilege."[121] Spock had sued the NSA as a target of warrantless surveillance, making claims for invasion of privacy under the Federal Tort Claims Act and New York law. The court refused to dismiss the case at the pleadings stage, saying the government's request for dismissal "goes beyond the traditional remedies fashioned by the courts in order to protect state secrets or other classified information."[122] The judge instead called for a "conference for the purpose of considering procedures to safeguard state secrets during this litigation."[123]

In the great majority of cases, courts have hesitated to even question the government. As Tom Blanton, Director of the National Security Archive observed, "[U]ntil a year or two ago, the judges rarely even questioned it when the government raised the 'state secrets' claim. It was a neutron bomb - no plaintiffs left standing."[124] As discussed in Part IV, as the government expands its invocation of the privilege (in terms of both the number of uses and the extent of the privilege's coverage) courts may wish to take a closer look at what secrets they are protecting.

---

119. United States Steel Corp. v. United States, 6 C.I.T. 182, 185 (1983).

120. Yang v. Reno, 157 F.R.D. 625, 635 (M.D. Penn. 1993) (holding that the executive secretary of the National Security Council was not considered competent to assert the privilege because he was not the head of a department, as required by *Reynolds*).

121. Spock v. United States, 464 F. Supp. 510, 519 (S.D.N.Y. 1978).

122. *Id.*

123. *Id.* at 520.

124. Eric Lichtblau, *U.S. Cites 'Secrets' Privilege as It Tries to Stop Suit on Banking Records*, N.Y. TIMES, Aug 31, 2007, at A17, *available at* http://www.nytimes.com/2007/08/31/us/nationalspecial3/31swift.html.

IV. INVOKING STATE SECRETS TO ACHIEVE GOVERNMENT IMMUNITY FOR A WIRETAP DRAGNET?

There are striking parallels between the government's disregard for laws regulating wiretapping during the Vietnam War and the government's disrespect for such laws today. The public's reaction, however, differs. The evolution of the statutes and case law discussed above came about in the face of both evolving technology and strong public opinion regarding illicit government spying. Perhaps the current "war on terrorism" differs from the Vietnam War in some respects. Maybe public opinion on the importance of privacy has diminished in an information age where online social sites, blogs, and web profiles keep very little personal information out of the public sphere. Whatever the reason, the public outrage responsible for pushing Congress to regulate wiretapping in the 1970s is not present to the same extent today.[125]

Perhaps in part because of the lack of public outcry over the government's most recent invasions into citizens' private communications, the state secrets privilege has been successfully expanding to become a tool for governmental immunity. With lessened public pressure on the legislature to step in and a judicial system that is willing to accept national security as a justification without closely examining the claimed secrets, the government may be able to use state secrets to escape necessary scrutiny of its wiretapping activities.

A. The Legality of the Alleged Wiretapping Activities in *Hepting*

Following *Keith*, the Church Report and the enactment of FISA in 1978, both Congress and the courts seemed to be sending a clear message that warrants were required to listen in on U.S. citizens' communications. Even before FISA, the Supreme Court's holding in *Keith* led Attorney General Richardson to curtail an NSA program targeting fewer than 600 Americans in order to avoid illegality.[126] If Richardson's understanding of *Keith* was correct, his reaction raises serious doubts about the legality of the much wider dragnet of spying alleged in *Hepting*. If the type of sur-

125. A Washington Post survey in May 2006 of about 500 American adults found that just 31% of Americans think respect for privacy is more important than investigating terrorist threats. The survey does imply an inverse relationship between privacy and security that has not necessarily been proven. The survey also found that 51% of Americans approve of the way Bush is protecting Americans' privacy rights and only 34% would be upset by if the government had kept track of all the phone calls they had made. *Washington Post-ABC News Poll*, WASH. POST, May 12, 2006, http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051206.htm.

126. See *infra* Section III.B for a further discussion.

veillance alleged in *Hepting* occurred without a warrant, it seems to clearly violate FISA, the Wiretap Act, and under *Keith*, the Fourth Amendment.

Indeed, Judge Walker's opinion took the view that *Keith*'s precedent, forbade the dragnet of surveillance alleged in *Hepting* in the absence of a warrant. Judge Walker expressly stated that "AT&T's alleged actions here violate[d] the constitutional rights clearly established in *Keith*,"[127] and that in *Keith*, "the Supreme Court held that the Fourth Amendment does not permit warrantless wiretaps to track domestic threats to national security."[128] Judge Walker also noted that the alleged dragnet passes through one of AT&T's "key domestic telecommunications facilities" and "it cannot reasonably be said that the program as alleged is limited to tracking foreign powers."[129] If such a dragnet is proven to exist at AT&T's domestic facility, all national security justifications presented by the government must fail under the *Keith* precedent.

Furthermore, given the FISC's liberality in doling out FISA warrants, there is little reason to believe that the court would have withheld certification from AT&T if the U.S. government's surveillance activities were, as the executive contends in public statements, limited to conversations of citizens who were communicating with people reasonably believed to be affiliated with al Qaeda. One might infer that the government's failure to obtain an FISC warrant for its surveillance activities on Folsom Street means that it was not *only* intercepting such communications. However, whether or not AT&T did or did not obtain a FISC warrant remains an unanswered question. Judge Pregerson asked at the Ninth Circuit *Hepting* oral arguments, "Was a warrant obtained in this case? You go through the FISA court on this case?"[130] The government's attorney replied, "Again, your honor, that gets into matters that are protected by the state secrets . . . whether it was or whether it was not. . . ." and later concluded, "I cannot say."[131]

---

127. Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 1010 (N.D. Cal. 2006).

128. *Id.*

129. *Id.*

130. Video: Oral Arguments in Hepting v. AT&T (C-SPAN television broadcast Aug. 15, 2007), Hepting v. AT&T, No. 06-17132 (9th Cir. Aug. 15, 2007), http://www.archive.org/details/gov.courts.ca9.2007.08.16 (last visited Apr. 5, 2008) [hereinafter "Oral Arguments"].

131. *Id.*

B. *Hepting* Exemplifies More Expansive Use of the State Secrets Privilege

The government, in facing these allegations of warrantless wiretapping, is not defending its actions based on compliance with FISA or the scope of Fourth Amendment protections. Instead, the government insists that the case must be dismissed under the state secrets privilege because it claims that judicial review of such claims would jeopardize national security. The state secrets privilege has been invoked in a number of wiretapping cases, both in the aftermath of the Vietnam War and recently.[132] The government, however, has recently enhanced its requests under the privilege; instead of using state secrets to hold back certain scientific evidence, it is asking that entire cases be dismissed.

One scholar has referred to the state secrets privilege as "the most powerful privilege available to the President" because it prevents disclosure of information to the courts and prevents a judicial check on the executive.[133] Also, given how superficial judicial review of state secrets claims has become, abuse of the privilege is far more likely. "The plain fact is that if department heads or the president know that assertion of the privilege is tantamount to conclusive on the judiciary, and that federal judges rarely order documents for inspection, then there is great incentive on the part of the executive branch to misuse the privilege."[134]

The courts do appear to be noticing the government's increasingly casual and abundant use of the privilege. The government attorney's refusal to answer Judge Pregerson's question about whether AT&T had government certification for its activities exemplifies the expansive use of the state secrets privilege. Judge Pregerson's response of "What's the problem?" is a hint at the court's growing unwillingness to accept "it's a secret" as an answer.[135] A District of Columbia district court also recently recognized the lack of government diligence when invoking the privilege, noting that although the government asserted the privilege "some 245 times" to avoid producing documents, they "totally failed to comply with the threshold [Reynolds] requirements" and at least one of the documents they sought to protect had already been produced in discovery.[136]

---

132. For cases subsequent to the Vietnam-era surveillance, see Halkin v Helms, 598 F.2d 1 (1978); Ellsberg v. Mitchell, 709 F.2d 51 (1983). For present day cases, see *Hepting*, 439 F. Supp. 2d 974 (2006); ACLU v. NSA, 493 F.3d 644 (2007).

133. Weaver, *supra* note 114, at 100.

134. *Id.* at 101.

135. *See* Oral Arguments, *supra* note 130.

136. Int'l Action Ctr. v. United States, 2002 U.S. Dist. LEXIS 16874 at *7-8 (D.D.C. 2002).

C. Abating the Privilege in *Hepting*

The holding of the Northern District of California in *Hepting* exhibits skepticism towards blanket use of the privilege, mirroring the ruling in *Spock*.[137] In *Hepting*, Judge Walker decided, after his in camera review of the secret materials, that the case could proceed. He recognized that state secrets might not allow *all* evidence to be presented, but decided to allow the case to proceed until, in light of the facts revealed during discovery, the plaintiff's case could not be made (or the defendants' defenses were actually precluded) due to a concealed state secret.[138] He refused to dismiss the case at the pleading stage and discussed procedures for determining the levels of security required by various materials.[139] In justifying his ruling, Judge Walker noted:

> It would be premature to decide these issues at the present time. In drawing this conclusion, the court is following the approach of the courts in *Halkin v Helms* and *Ellsberg v Mitchell*; these courts did not dismiss those cases at the outset but allowed them to proceed to discovery sufficiently to assess the state secrets privilege in light of the facts.[140]

The pair of *Halkin* cases (*Halkin I* and *II)* and *Ellsberg* were wiretapping cases that followed the Vietnam War. At that time, revelations about the government's practically unlimited ability to wiretap and citizens' outraged responses created litigation, led to the Church Report, and induced Congress to pass FISA.[141] Amid this post-Vietnam response, the *Halkin* cases and *Ellsberg* each examined the government's right to wiretap without a warrant. The cases also grappled with a key question left open by *Reynolds*: how much scrutiny should be given to a government claim of privilege?

The cases treat government assertions of the state secrets privilege with remarkably different levels of deference when applied to warrantless surveillance. While the *Ellsberg* decision did advocate judicial review of government claims of secrecy, the two *Halkin* cases seemed to actually expand the level of discretion given to the government to shield evidence

---

137. Spock v. United States, 464 F. Supp. 510, 519 (S.D.N.Y. 1978) (holding that the state secrets privilege "should be construed narrowly" and progressing with the litigation with plans to safeguard any state secrets.).

138. *Hepting*, 439 F. Supp. 2d at 995.

139. *Id.* at 1010.

140. *Id.* at 994.

141. *See* Sales, *supra* note 43, at 814.

as a state secret.[142] What they have in common, as Judge Walker notes, is that neither court dismissed the case; instead, each only barred the discovery of certain evidence.[143]

1. The Halkin *Cases*[144]

In *Halkin I*, the district court stated that "[c]ourts should accord the 'utmost deference' to executive assertions of privilege upon grounds of military or diplomatic secrets."[145] The court need only be satisfied that 'there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged.'"[146] As a result of this standard, the court in *Halkin I* allowed the government to invoke the privilege and withhold the requested evidence.

Dissenting from the ensuing denial of rehearing en banc, two D.C. Circuit judges argued that the court failed to consider the countervailing interests in disclosure of the secret information—as *Reynolds* required.[147] The judges went on to deride the panel for failing to consider the Supreme Court's holding in *Keith* which "erect[ed] firm limits on the authority of the executive to conduct warrantless surveillance, even in the name of national security."[148] Finally, the dissenting judges noted the danger of giving the executive branch such great deference to declare un-examined evidence a secret:

---

142. Halkin v. Helms, 598 F.2d 1 (D.C. Cir. 1978) (*Halkin I*); Halkin v. Helms, 690 F.2d 997 (D.C. Cir. 1982) (*Halkin II*); Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983).

143. *Hepting*, 439 F. Supp. 2d at 993.

144. In *Halkin I*, 27 individuals and organizations who actively opposed the war in Vietnam sued the NSA, the FBI, and other government employees, claiming that they were the subjects of warrantless surveillance. In this action, plaintiffs were attempting to compel discovery of certain information that could prove their case, but the government refused to provide the requested documents. Some facts about the surveillance programs had already come to light by way of the press and a presidential commission on intelligence activities (the Rockefeller Commission). The government invoked the state secrets privilege and claimed that admitting or denying the acquisitions of the plaintiffs' communications would reveal important military and state secrets regarding the capabilities of the NSA to collect and analyze foreign intelligence. *See Halkin I*, 598 F.2d at 3. *Halkin II* was an appeal that came after the court's refusal to compel the information led to the plaintiff's case being dismissed. *See Halkin II*, 690 F.2d 997.

145. *Halkin I*, 598 F.2d at 9.

146. *Id.*

147. *Id.* at 12 ("Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted . . . ." (quoting United States v. Reynolds, 345 U.S. 1, 11 (1953))).

148. *Id.* at 13.

> The "utmost deference" which the panel has given the government's Ex parte, in camera assertions is not justified in precedent, conflicts with other decisions of this court . . . and slights the role of the court in protecting the civil liberties guaranteed by the Fourth Amendment.[149]

The dissenting judges declared, "the privilege becomes a shield behind which the government may insulate unlawful behavior from scrutiny and redress by citizens who are the target of the government's surveillance."[150]

The *Reynolds* decision was partially responsible for the difficult position the *Halkin* court faced because the *Reynolds* Court did not clearly delineate when a document should be examined in camera. "The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect."[151] Unable to articulate how to make this decision, the *Reynolds* Court relied on analogy, comparing it to the standard required for a witness who wishes to avoid giving testimony that he claims will incriminate him.[152] Should the witness have to share the testimony with the court to confirm that it is, in fact, incriminating? Or should the court always accept a witness's bare assertion of the privilege? The *Reynold*s Court determined that, when formulating the balance between requiring the government's full disclosure and accepting the government's bare assertion of the state secrets privilege, a court may not necessarily require disclosure. At the same time, the Court expressly disclaimed the extreme of accepting the government's assertion on its face.[153]

The *Reynolds* Court advocated something more than acceptance of a bare assertion but something less than requiring full disclosure. But what is that *something more*? What beyond a mere claim of privilege satisfies the court "that a responsive answer to the question or an explanation of why it cannot be answered might be dangerous"?[154] In the *Halkin* cases, the satisfaction seemed to spring from the government's fulfilling the three formal procedural requirements set out in *Reynolds* and some additional

149. *Id.* at 14.

150. *Id.* at 13-14.

151. United States v. Reynolds, 345 U.S. 1, 8 (1953).

152. *Id.*

153. *Id.* Analogizing to the question of how much disclosure should be required to invoke the privilege against self-incrimination, the Court observed that despite "some saying that the bare assertion by the witness must be taken as conclusive, and others saying that the witness should be required to reveal the matter behind his claim of privilege to the judge for verification. . . . Neither extreme prevailed." The Court reasoned that "some like formula of compromise must be applied here." *Id.*

154. *Id.* at 9.

statements from the executive appearing in an in camera affidavit. In camera review of the actual evidence was not required, although it is questionable whether reading an affidavit and accepting a government official's word should qualify as a judicial check on the executive.

In *Halkin II*, the plaintiffs appealed the dismissal of their case that came as a result of the withheld evidence.[155] Regarding state secrets, the appellants only made procedural arguments, about the government's method of invoking the privilege. According to the court:

> Since that ruling resulted in maintaining the secrecy of the information sought, it is scarcely surprising that appellants have not chosen to contest the sensitivity of the information on its merits. Even had they the means and the desire to do so, our task would be no different, for the standard set down in *Reynolds* is itself *purely a procedural framework for testing claims of privilege.*[156]

The court went on to say that beyond ensuring that the procedural requirements are met, *Reynolds* requires that "the court must be satisfied from all the evidence and circumstances . . . that a responsive answer to or an explanation of why it cannot be answered might be dangerous because injurious disclosure might result."[157] However, it is not clear how this satisfaction—that the answer or explanation was harmful—was gained in *Halkin*. The court reviewed an in camera affidavit from the director of the CIA,[158] but never examined the evidence that the government sought to withhold. The court took the government at its word that the "'seemingly innocuous' information [could be] part of a classified 'mosaic' that 'can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate.'"[159] Once an agent of the executive met the formal *Reynolds* requirements, and attested to the secrecy of the evidence in an affidavit, the court accepted the privilege.

Halkin II seemed to further expand the executive's discretion and dilute chances for judicial review, saying, "Secrets of state . . . are absolutely privileged from disclosure in the courts. . . . Once the court is satisfied that the information poses a reasonable danger to secrets of state, *even the most compelling necessity cannot overcome the claim of privilege.*"[160] Here the

155. Halkin v. Helms, 690 F.2d 997, 997 (D.C. Cir. 1982) (*Halkin II*).
156. *Id.* at 991 (emphasis added).
157. *Id.*
158. *Id.* at 986.
159. *Id.* at 993.
160. *Id.* at 990 (emphasis added).

court severely minimizes the *Reynolds* requirement that a court look for a "showing of necessity" to "determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate."[161] This was in spite of the fact that the necessity of the evidence in the *Halkin* case was great. Following the court's refusal to compel the discovery, the case was dismissed because it lacked evidence that such discovery might have provided.[162]

2. The Ellsberg *Case*

Ellsberg v. Mitchell, the other case relied on in *Hepting* for allowing plaintiffs to proceed to discovery, indicated much more stringent treatment of the state secrets privilege.[163] The court in *Ellsberg* insisted on in camera review when the government's claim of secrecy was dubious and served to end its opponent's law suit.[164] The court discussed how to determine "whether (and in what spirit) the trial judge in a particular case should examine the materials sought to be withheld," noting "[w]hen a litigant must lose if the claim is upheld and the government's assertions are dubious in view of the nature of the information requested and the circumstances surrounding the case, careful in camera examination is not only appropriate *. . . but obligatory . . .*"[165]

The in camera review of the evidence caused the court in *Ellsberg* to determine that the materials were properly withheld.[166] However, like *Halkin*, the court did not dismiss the case, but merely refused to compel the requested discovery.[167] In both cases, despite showing different levels of deference for the executive's assertion of the privilege (*Ellsberg* called for "considerable deference" as opposed to "utmost deference"[168]) the court denied access to evidence but allowed the trial to proceed.

---

161. United States v. Reynolds, 345 U.S. 1, 11 (1953).

162. *See Halkin II*, 690 F.2d at 987.

163. *See* Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983). *Ellsberg* is a civil case following by criminal proceedings pertaining to the Pentagon Papers litigation. Plaintiffs in *Ellsberg* (defendants, their attorneys, and advisors from the criminal cases) claimed that over the course of the criminal proceedings at least one of them was the subject of warrantless wiretapping. *Id.* at 52-53. The discovery in the civil case was disrupted by a government claim of the state secretes privilege and buttressed by a declaration from the Attorney General and a sealed evidentiary exhibit provided to the district court for in camera review. *Id.* at 54.

164. *Id.* at 59.

165. *Id.* (internal citations omitted) (emphasis added).

166. *Id.* at 52.

167. *Id.* at 59.

168. *Id.* at 58.

Judge Walker's decision in *Hepting* reflects skepticism of the state secrets doctrine, as well as awareness of the potential for abuse and the court's obligations to protect civil liberties—themes present in *Ellsberg*[169] and the *Halkin* dissent, although absent in *Halkin II*. *Ellsberg* is the key precedent that Judge Walker relies upon in *Hepting*. While some evidence may be withheld based on the state secrets privilege and that withheld evidence may result in dismissal of the case, the privilege itself should not automatically call for dismissal of the case as long as privileged evidence can be disentangled from non-privileged evidence.[170] Additionally, Judge Walker's decision to allow *Hepting* to proceed to discovery parallels the dissenting judge's response to the D.C. Circuit's refusal to rehear *Halkin I* en banc.[171] Like the dissenting judges in *Halkin*, the court in *Hepting* recognized that "[w]here there is a strong showing of necessity, the claim of privilege should not be lightly accepted" and notes that "AT&T's alleged actions here violate the constitutional rights clearly established in *Keith*."[172] Judge Walker's decision properly rejects the view that *Reynolds* requires only procedural hurdles that can be overcome by bare assertions and instead preserves the balancing test that *Reynolds* suggested.

V. THE DANGER OF EXPANDING THE STATE SECRETS PRIVILEGE

A. Expansion of the State Secrets Doctrine in Non-Wiretap Cases

In recent years, the use of the state secrets privilege has been expanding, both in frequency of use and in the types of protection it provides. Rather than simply serving as an evidentiary privilege to keeping secret documents out of discovery, the privilege has been more frequently invoked in order to dismiss entire cases—a far more serious denial of access to the courts. This non-justiciability application of the doctrine has previously been invoked in cases where the presence of state secrets is clear and all parties involved in the dispute entered into the scenario with full knowledge of the secrecy required.[173] More recently, the government has

169. *Id.* at 59.

170. *Id.* at 57 ("The privilege may not be used to shield any material not strictly necessary to prevent injury to national security; and whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.").

171. Halkin v. Helms, 598 F.2d 1, 11 (D.C. Cir. 1978) (*Halkin I*).

172. Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 982, 1010 (N.D. Cal. 2006)

173. *See, e.g.*, Tenet v. Doe, 544 U.S. 1, 9 (2005) (attempting to enforce an espionage contract with government); Weinberger v. Catholic Action of Haw./Peace Educ. Project, 454 U.S. 139, 146-47 (1981) (attempting to force publication of environmental impact

attempted to invoke the non-justiciability application in situations where the government is accused of blatant wrongdoing against innocent individuals. Furthermore, as exemplified in *Hepting*, the government seeks not to exempt evidence or hold an in camera trial, but to entirely avoid defending its actions. In *Reynolds*, the government only invoked the state secrets privilege to shield certain evidence from discovery; the courts allowed the case as a whole to proceed. In *Hepting*, by contrast, the government is invoking the non-justiciability application in order to dismiss the entire case at the outset.

The government has recently invoked the state secrets privilege to dismiss several cases filed in response to the "extraordinary rendition" program.[174] In *El-Masri* a German citizen claimed the CIA kidnapped, tortured and interrogated him after mistaking him for a terrorist with a similar name.[175] The Fourth Circuit upheld the district court's decision to dismiss the case at the pleading stage under the state secrets privilege, saying that "the judiciary's role as a check on presidential action in foreign affairs is limited."[176] Like the court in *Halkin*, the Fourth Circuit accepted an affidavit from the executive explaining why the evidence could not be released; however, the court held that if "an explanation by the executive of why a question cannot be answered would itself create an unacceptable danger of injurious disclosure, the court is obliged to accept the executive branch's claim of privilege without further demand."[177] Here, the court allowed for the possibility that not only can the executive withhold evidence from trial, but it can also withhold it from in camera review *and* it is not even required to explain *why* it withholds the evidence if the executive merely states that such an explanation would be damaging to national security.

This logic allowed the executive to force the dismissal of the lawsuit of a potentially innocent man who claims the government conspired to kidnap and torture him because of a case of mistaken identity. The privilege here is not only ending valid litigation on the government's word—it

---

report on the storage of nuclear weapons); Totten v. United States, 92 U.S. 105, 107 (1875) (attempting to enforce espionage contract with government).

174. For the government's use of the state secrets privilege to prevent trials on two extraordinary rendition detainees, *see* El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007), *cert. denied,* 128 S. Ct. 373 (2007), Arar v. Ashcroft, 414 F. Supp. 2d 250 (E.D.N.Y. 2006). Here, though the government asserted state secrets to dismiss the case, the court found the state secrets issue moot because it was able to dismiss all counts on other grounds. As this Note went to press, the case was on appeal to the Second Circuit.

175. *See* El-Masri v. Tenet, 437 F.Supp. 2d 530, 536 (E.D. Va. 2006).

176. *See* El-Masri v. United States, 479 F.3d at 303.

177. *Id.* at 305-306.

is killing litigation filed in response to claims of *criminal* behavior by the government. *El-Masri* is not the only recent case to have faced complete dismissal prior to discovery following the invocation of the state secrets privilege—it has also been invoked, for example, to end litigation over government employees' claims of wrongful conduct in the workplace.[178] In comparison to the results in *Halkin*, *Ellsberg*, and *Reynolds*, where privileged evidence was singled out and withheld, these cases of dismissal create a serious denial of the court system and shield questionable government activities from scrutiny.

Coupled with the expansion of the *way* the government is using the privilege is the sheer increase in *volume* of the privilege's invocation.[179] The Bush administration's attorneys have invoked the privilege more than any other president in the nation's history.[180]

As the executive's use of the privilege increases, courts may become more willing to question the facts underlying the invocations. The Ninth Circuit, most recently, seemed inclined to question how much deference the executive should be given. Judge Pregerson asked the government's attorney during *Hepting* oral arguments, "[A]re you saying the courts are to rubber stamp the determination that the executive makes that there's a state secret?"[181] The Ninth Circuit panel seemed mindful of both the history of government misuse of wiretaps and the expansive use of the state secrets privilege to purge litigation that questions government wrongdoing, especially in times of war.[182]

---

178. *See, e.g*, Edmonds v. United States Dep't of Justice, 323 F. Supp. 2d 65 (D.D.C. 2004). In *Edmonds*, plaintiff's claims of retaliation following the loss of her job due to reporting alleged FBI misconduct were dismissed after the government invoked the state secrets privilege to withhold a classified declaration that supported her claim. The court held that without it she would be unable to prove the prima facie elements of her case. *See also* Tilden v. Tenet, 140 F. Supp. 2d 623 (E.D. Va. 2000) (dismissing sex discrimination action against Central Intelligence Agency because there was no way the lawsuit could proceed without disclosing state secrets).

179. *See* Scott Shane, *Invoking Secrets Privilege Becomes a More Popular Legal Tactic by U.S.*, N.Y. TIMES, June 4, 2006 at 32, *available at* http://www.nytimes.com/2006/06/04/washington/04secrets.html.

180. *Id.*

181. *See* Oral Arguments, *supra* note 130.

182. Judge Pregerson, for example, asked government council, "I mean, is it the government's position that when our country is engaged in a war that the power of the executive when it comes to wiretapping is unchecked?" Oral Arguments, *supra* note 130.

B. The State Secrets Privilege in the Future

Although courts have historically been reluctant to question government assertions of secrecy,[183] the increase in the number of assertions of the privilege should make courts cautious. The government's efforts toward expanding the state secrets privilege—from an exceptional standard of evidentiary privilege into a rule depriving citizens of recourse against their government's wrongful conduct—is creating an overbroad policy of immunity for the government out of what was once a narrow evidentiary rule. The court in *El-Masri* seemed to support this expansion of the privilege by noting that "to the extent an executive claim of privilege 'relates to the effective discharge of a President's powers, it is constitutionally based.'"[184] However, the *El-Masri* court overlooked the fact that in upholding the President's supposed constitutional power, it denied the plaintiff's constitutional right of access to the court.

The outcome of *Hepting* may provide an answer about how much deference courts will be willing to give the executive in the future when the state secrets privilege is asserted. The adherence to a mere "procedural framework" endorsed in *Halkin* encountered serious questions when *Hepting* was argued before the Ninth Circuit.[185] Rather than allowing a request from the executive to end the lawsuit, the Ninth Circuit may instead call for the privilege to be used more narrowly—to only eliminate such evidence as will actually protect national security.[186] Judge Pregerson, for one, seemed to indicate that the district court judge should consider whether individual evidence was privileged or not. When AT&T's lawyer

---

183. Steve Aftergood of the Federation of American Scientists points out on his Secrecy News Blog, "Although the executive branch's assertion of the state-secrets privilege has been denied by judges on at least four occasions . . . those denials seem to have been based on technical defects or procedural failings rather than a substantial judicial assessment of the merits. . . ." Posting of Steve Aftergood to Secrecy News, Court Denies State Secrets Claim in Wiretapping Case, http://www.fas.org/blog/secrecy/2008/ 04/us_ intelligence_agencies.html (July 21, 2006 11:55 EST). *See also* discussion, *infra* Section III.C.

184. El-Masri v. United States, 479 F.3d 296, 303 (4th Cir. 2007) (quoting United States v. Nixon, 418 U.S. 683, 711 (1974)).

185. Judge McKeown noted that disallowing discovery based purely on government assertions "put us in the position of being in the 'trust us' category." Oral Arguments, *supra* note 130.

186. Judge Hawkins, discussed the state secrets privilege's ordinary procedure, "Ordinarily in a piece of litigation where there is some contention that state secrets may be involved, the ordinary course . . . would be to let the litigation go forward and as the government asserts the privilege, the Article III district judge looks at the information in camera and then makes that determination . . . ." He then asked, "Why wouldn't that work here?" Oral Arguments, *supra* note 130.

noted that the government's invocation of the privilege tied their hands as far as providing a valid defense, Pregerson said, "That'll be something Judge Walker will have to look into in the future, I suppose."[187]

C. The Importance of In Camera Review

The Ninth Circuit, in questioning whether executive affidavits explaining why evidence cannot be released could serve as a judicial check, may reinvigorate the importance of in camera reviews.[188] The Supreme Court said in *Reynolds*, thirty years before the Vietnam War and more than seventy years before September 11, "[W]e will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case . . . ."[189] Since *Reynolds*, courts have only required in camera review of the documents at issue in about one-third of reported cases where the privilege has been invoked.[190] Since the presidency of George H.W. Bush, the privilege has been invoked in at least twenty-three reported cases, but in only five of those cases did a court require in camera review of the allegedly secret evidence.[191] In determining whether to enforce in camera reviews, courts must remember that "it is costless for the president to assert a secrecy privilege: the overwhelming odds are that the assertion will be successful, and even if unsuccessful, the process of overturning claims of privilege is lengthy and the only potential cost of excessive claims of national security is in bad publicity."[192]

The United States has participated in unpopular wars twice since *Reynolds* was decided. During each war the government likely exceeded the boundaries of legality in order to surveil the communications of its own citizens. The government has done this in spite of laws that clearly prohibit domestic surveillance without a warrant. During and following both wars, litigation arose and the government attempted to hide its illegal behavior by invoking the state secrets privilege. The state secrets privilege

---

187. Oral Arguments, *supra* note 130.

188. Judge Pregerson asked, "But what are the checks on it? If we're getting affidavits from folks in the executive branch and we have to take their word for it, what is the check?" Oral Arguments, *supra* note 130.

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

190. Weaver, *supra* note 114, at 101.

191. *Id.* Note this article was published in 2005. The Washington Post has since noted that George W. Bush has invoked the privilege, himself, 23 times since September 11, 2001. Dana Priest, *Secrecy Privilege Invoked in Fighting Ex-Detainee's Lawsuit*, WASH. POST, May 13, 2006 at A03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/05/12/AR2006051202008.html.

192. Weaver, *supra* note 114, at 86.

has been very successful in blocking inquiry into government wrongdoing in large part because the judiciary has relinquished much of its power for judicial review in response to *Reynolds.* In attempting to apply *Reynolds*, courts have repeatedly passed over in camera review of allegedly secret evidence in favor of trusting the executive's claims of national security concerns. Given the executive's historic misuse of the privilege, courts must begin re-employing in camera review to ensure that the government is not abusing the doctrine to cover up further wrongdoing. The Ninth Circuit has the opportunity to disallow such broad, abuse of the privilege by altering the precedent on federal court review of government assertions of secrecy.

Allowing the automatic dismissal of cases such as *Hepting* will not enhance national security. The EFF, plaintiffs' council in *Hepting*, has compiled a list of forty-eight court cases where national security was at issue and federal district court judges securely handled documents ex parte and in camera.[193] In *Hepting*, after examining the disputed documents, Judge Walker found it would be possible to shield information detrimental to national security without completely forsaking the plaintiffs' right to air their grievances against the government.[194] He stated, "[t]he compromise between liberty and security remains a difficult one. But dismissing this case at the outset would sacrifice liberty for no apparent enhancement of security."[195] In making this statement, Walker apparently rejected the non-justiciability approach of allowing the executive to shut down litigation based on their bare assertion that the very subject matter of the case is a state secret.

Khalid El-Masri, Sibel Edmonds, and the other aggrieved individuals like them whose lawsuits against the government were eliminated by the state secrets privilege have a right to their day in court if it is at all possible to provide it without putting the country at risk. *Reynolds* created the process of balancing citizens' right to trial and the nation's security.[196] This method of balance has been advocated by both *Ellsberg* and the dis-

193. Electronic Frontier Foundation, No National Security Information has ever Leaked from Federal Courts in more than 50 years of FISA and States Secrets Cases; Congress Can Trust Them Fully in the Pending Cases (2007), *available at* http://www.eff.org/files/nsa/courts.pdf.

194. Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 995 (N.D. Cal. 2006) ("To defer to a blanket assertion of secrecy here would be to abdicate that duty [to adjudicate disputes].").

195. *Id.*

196. *See* United States v. Reynolds, 345 U.S. 1, 9-10 (1953).

senting judges in *Halkin I*.[197] These cases support Judge Walker's assessment that liberty and security must be balanced when the state secrets privilege is asserted. When the government's assertion of the privilege is questionable, in camera review of the evidence (not just an affidavit from the government) is the best tool courts have to make the compromise between liberty and security. As the court said in *Halpern* (where the court held an entire trial in camera to balance security and liberty), the state secret privilege does not apply "when disclosure to court personnel in an in camera proceeding will not make the information public or endanger the national security."[198]

At minimum, federal judges have a duty to examine the materials the government seeks to withhold and determine if a fair trial is possible. The Supreme Court has itself noted that when there is doubt, the court should use the tools at its disposal, including in camera review, to determine what materials should be withheld and what may be disclosed.[199]

VI. CONCLUSION

In the aftermath of September 11, 2001, the federal government has been repeatedly accused of wrongful conduct against individuals. When those individual brought suit, rather than defend its conduct, the government invoked the state secrets privilege. Courts have a responsibility to engage in judicial scrutiny of government claims of privilege and provide citizens with an avenue for redress if at all possible. Judges should not allow the mere utterance of the phrase "state secrets" to end litigation.

When it established the state secrets privilege in *Reynolds*, the Supreme Court said, "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers."[200] The question remains: how, by allowing a mere affidavit to end litigation and cover up the government's own wrongdoing; how, given the government's historic temptation to invoke the privilege when it is more convenient or less embarrassing than admitting the truth; how, without requiring in camera review and merely taking the word of the executive; how, then can the judicial control *not* be abdicated to the caprice of the executive?

---

197. *See* Ellsberg v. Mitchell, 709 F.2d 51, 59 (D.C. Cir. 1983); Halkin v. Helms, 598 F.2d 1, 12 (D.C. Cir. 1978) (*Halkin I*).

198. Halpern v. United States, 258 F.2d 36, 44 (2d Cir. 1958).

199. Kerr v. U.S. Dist. Court, 426 U.S. 394, 405-06 (1976) ("[T]his Court has long held the view that in camera review is a highly appropriate and useful means of dealing with claims of governmental privilege.").

200. *Reynolds*, 345 U.S. at 9-10.