1-1-2008

The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States

Michael Avery

The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States

MICHAEL AVERY*

I. INTRODUCTION

In the fall of 2001, shortly after the terrorist attacks of September 11, the National Security Agency ("NSA") launched a secret program to engage in electronic surveillance, without prior judicial authorization, of communications between persons in other countries and persons inside the United States (the "Terrorist Surveillance Program" or "TSP").[1]

* Professor, Suffolk Law School, Boston, Massachusetts. I am grateful to the deans of Suffolk Law School for a summer-writing stipend that made this article possible and to my research assistant, Suzanne Manning, for her invaluable assistance in the preparation of the final draft of this article. It is important to disclose that I am one of the lawyers representing the plaintiffs in *Center for Constitutional Rights v. Bush*, No. 06-CV-313 (S.D.N.Y. filed Jan. 17, 2006), which is currently pending before the Honorable Vaughn R. Walker in the U.S. District Court for the Northern District of California. I do so on behalf of the National Lawyers Guild. As such I have a strong bias in favor of the argument that the government's actions with respect to warrantless electronic surveillance have been in violation of federal statutes and of the Constitution. In addition, it is important to acknowledge that this article is heavily dependent, including for some of its language, on the briefing that we have done in that case. The plaintiffs' briefs were prepared by a team of lawyers, including in addition to me, Professor David Cole from Georgetown Law School, Shayana Kadidal from the Center for Constitutional Rights ("CCR"), Ashlee Albies from Portland, Oregon, and Bill Goodman from Detroit, Michigan (formerly the Legal Director at CCR). The briefs were written through the exchange of drafts and redrafts of various sections and numerous conferences among the five lawyers and were very much a collective effort. Mr. Kadidal played a particularly pivotal role in coordinating this process and in preparing the final drafts of briefs for filing. In addition, we had available and we relied on drafts of briefs filed at various points by lawyers for the American Civil Liberties Union ("ACLU") in *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), and by the lawyers for the plaintiffs in *Al-Haramain Islamic Foundation, Inc. v. Bush*, 451 F. Supp. 2d 1215 (D. Or. 2006). The plaintiffs' counsel in *Center for Constitutional Rights v. Bush* have also had numerous conferences with the lawyers from the Electronic Frontier Foundation representing the plaintiffs in *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006). I am indebted to my colleagues for their collective wisdom, although any errors that may exist in this article are my sole responsibility.

1. Much of what the government has disclosed about the TSP is set forth in *Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190 (9th Cir. 2007); *see also* James Taranto, *The Weekend Interview with Dick Cheney: A Strong Executive*, WALL ST. J., Jan. 28, 2006, at A8 ("[Cheney explains the program as] 'the interception of communications, one end of which is outside the United States, and one end of which, either outside the U.S. or inside, we have reason to believe is al-Qaeda-connected.'"); Gen. Michael V. Hayden, What American Intelligence and Especially the NSA Have Been Doing To Defend the Nation, Address to the National Press Club (Jan. 23, 2006), *available at* http://www.dni.gov/speeches/20060123_speech.htm [hereinafter Hayden, *Press Club*] (acknowledging that the NSA Program covers international calls); Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael

Despite the clear language of the Foreign Intelligence Surveillance Act ("FISA")[2] and of Title 18 of the United States Code[3] that no electronic surveillance was permitted other than that authorized by statute, the President claimed inherent power to conduct such surveillance. And despite the clear intent of Congress that the President should seek an amendment to FISA to authorize extraordinary surveillance lasting more than fifteen days during wartime,[4] the President did not seek such an amendment and instead acted unilaterally and in secret. President Bush reauthorized the TSP, again in secret, multiple times, and originally intended to continue doing so indefinitely.[5]

The electronic surveillance conducted by the NSA on the orders of the President raised serious constitutional questions concerning the separation of powers and the scope of protection provided by the warrant requirement of the Fourth Amendment. These issues quickly became the subject of litigation as several lawsuits were filed to try to enjoin the program or obtain damages for persons who had been subjected to warrantless electronic surveillance.[6] The government moved to dismiss the suits on the ground that the cases could not be litigated without the dis-

---

Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html [hereinafter Gonzales/Hayden, *Press Briefing*] ("The President has authorized a program to engage in electronic surveillance . . . ."); President's News Conference, 41 WEEKLY COMP. PRES. DOC. 1885 (Dec. 19, 2005) (noting that "calls" are intercepted); President's Radio Address, 41 WEEKLY COMP. PRES. DOC. 1880, 1881 (Dec. 17, 2005) ("In the weeks following the terrorist attacks on our Nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to Al Qaida and related terrorist organizations.").

2. 50 U.S.C. § 1801–1862 (2000).

3. 18 U.S.C. § 2511(2)(f).

4. 50 U.S.C. § 1811.

5. President's News Conference, *supra* note 1, at 1885 ("I've reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for so long as our Nation is—for so long as the nation faces the continuing threat of an enemy that wants to kill American citizens.").

6. *See, e.g.*, ACLU v. NSA, 438 F. Supp. 2d 754, (E.D. Mich. 2006), *vacated*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, No. 07-468, 2008 WL 423556, at *1 (U.S. Feb. 19, 2008); Al-Haramain Islamic Found., Inc. v. Bush, 451 F. Supp. 2d 1215, 1218 (D. Or. 2006), *rev'd*, 507 F.3d 1190 (9th Cir. 2007); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 979 (N.D. Cal. 2006); Ctr. for Constitutional Rights v. Bush, No. 06-CV-313 (S.D.N.Y. filed Jan. 17, 2006). One important issue in these cases is the standing of the plaintiffs to challenge the electronic surveillance program. Other than in *Al-Haramain*, there is no evidence that any particular plaintiffs were in fact subjected to surveillance. Plaintiffs in the *Center for Constitutional Rights* and *ACLU* cases alleged that they had standing because their professional responsibilities required them to communicate with persons who were suspected of being members of al Qaeda, or otherwise likely to be targets of the TSP, and that they were required to alter their behavior as a result of the risk of having privileged communications overheard by the government. The Sixth Circuit rejected the ACLU plaintiffs' standing argument in *ACLU v. NSA*, 493 F.3d 644, 648 (6th Cir. 2007), *cert. denied*, No. 07-468, 2008 WL 423556, at *1 (U.S. Feb. 19, 2008).

closure of state secrets.[7] The government then successfully moved to consolidate most of the cases through the multidistrict-litigation panel.[8]

The government has been remarkably successful at avoiding any definitive resolution of the constitutional issues in this controversy. At the time of this writing, court decisions have been rendered on some of the preliminary issues raised by the cases,[9] and one district judge has addressed the merits and issued an injunction against the government,[10] although that decision was vacated on appeal on the ground that the plaintiffs did not have standing to challenge the program.[11] But it is unclear when, if ever, the U.S. Supreme Court will confront the question of the President's power to conduct warrantless electronic surveillance of foreign threats to national security. By way of comparison, in the case that is the closest parallel with respect to the constitutional issues, President Harry Truman issued an executive order during the Korean War seizing the steel mills on April 8, 1952, the suit challenging his actions was argued in the Supreme Court on May 12 and 13, 1952, and the Court issued its decision concluding the President lacked the power to make the seizure on June 2, 1952.[12]

Part II of this article provides the history of the Bush administration's warrantless electronic surveillance after September 11, 2001.

Part III lays out the statutory framework that existed under FISA. It discusses the principal arguments concerning the question whether the President has inherent power to conduct warrantless electronic surveillance of suspected foreign threats to national security. This section argues that in the face of Congress's clear decision that such surveillance required a judicial warrant, the President had no inherent authority to engage in surveillance without a warrant. The section also discusses and rejects the government's argument that the Authorization for the Use of Military Force ("AUMF"), issued by Congress following September 11, impliedly authorized the TSP.

Part IV discusses the state-secrets privilege and the question whether the judicial branch may entertain challenges to the TSP in the

7. *See* discussion *infra* Part III on state secrets. The issue arose in different ways in the various cases. In *Center for Constitutional Rights*, plaintiffs moved for summary judgment before any discovery was conducted and took the position that no discovery was necessary. The CCR plaintiffs argued that the statutory and constitutional issues in the case could be decided on the basis of the public record.

8. Transfer Order at 1–3, *In re* NSA Telecomms. Records Litig., No. 06-1791, 2007 WL 3306579 (N.D. Cal. Nov. 6, 2007).

9. *See* Al-Haramain Islamic Found., 507 F.3d at 1203–04; *Hepting*, 439 F. Supp. 2d at 979–80.

10. *ACLU*, 438 F. Supp. 2d at 782.

11. *ACLU*, 493 F.3d at 687–88.

12. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

face of the assertion of that privilege. It argues that the courts must determine the constitutionality of the TSP by reference to first principles and that state secrets are not essential to that inquiry. This argument is buttressed by the fact that the Supreme Court has resolved other significant constitutional controversies and that the existence of "state secrets" has not been a bar to the Court's ability to resolve bedrock separation-of-powers issues.

Part V discusses the change in the Bush administration's strategy in January 2007 when it sought and obtained orders from the Foreign Intelligence Surveillance Court ("FISA Court" or "FISC") authorizing electronic surveillance that had been conducted previously through the TSP. It argues that this change did not render moot the legal challenges pending to the TSP.

Part VI addresses the question of the constitutionality of the amendments to FISA that were enacted in August 2007. It concludes that even as authorized by Congress, warrantless electronic surveillance violates the Fourth Amendment. In particular, the article rejects the government's assertion that the special-needs exception to the Fourth Amendment justifies this surveillance.

The article concludes that warrantless electronic surveillance under the TSP was beyond the President's powers under Article II, given Congress's clear proscription of such surveillance. It further concludes that warrantless electronic surveillance is beyond the powers of the federal government even with Congressional approval, owing to the warrant requirement of the Fourth Amendment.

II. THE HISTORY OF THE TERRORIST SURVEILLANCE PROGRAM

As part of the TSP,[13] NSA targeted for interception "calls . . . [the government has] a reasonable basis to believe involve al Qaeda or one of its affiliates."[14] NSA also targeted the communications of individuals it deemed suspicious on the basis of NSA's belief that the targeted individuals had some unspecified "link" to al Qaeda or unspecified related terrorist organizations,[15] that they belonged to an organization that the

13. On two occasions since its inception, the government has acknowledged changing the program in significant ways. The program became a moving target in the face of litigation challenging the constitutionality of this electronic surveillance, and in the face of occasional congressional criticism. The history of the program is described in this introduction.

14. Hayden, *Press Club*, *supra* note 1.

15. President's News Conference, *supra* note 1, at 1885 ("I authorized the interception of international communications of people with known links to Al Qaida and related terrorist organizations."); President's Radio Address, *supra* note 1, at 1881 ("Before we intercept these communications, the Government must have information that establishes a clear link to these terrorist networks."); Taranto, *supra* note 1 ("[Cheney explains the program as] 'the interception of communications, one end of which . . . we have reason to believe is al-Qaeda-connected.'");

government considers to be "affiliated" with al Qaeda,[16] that they had provided some unspecified support for al Qaeda,[17] or that they "want to kill Americans."[18] Information collected under the program was sometimes retained and sometimes disseminated.[19] The Attorney General refused to specify the number of Americans whose communications have been or are being intercepted under the TSP.[20]

NSA intercepted communications under the TSP without obtaining a warrant or judicial authorization.[21] Apparently, neither the President

---

Attorney General Alberto Gonzales, Ask the White House (Jan. 25, 2006), http://www.whitehouse.gov/ask/20060125.html ("[The NSA intercepts] international communications involving someone we reasonably believe is associated with al Qaeda . . . ."); Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, U.S. Dep't of Justice, to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, John D. Rockefeller, IV, Vice Chairman, Senate Select Comm. on Intelligence, Peter Hoekstra, Chairman, Permanent Select Comm. on Intelligence, and Jane Harman, Ranking Minority Member, Permanent Select Comm. on Intelligence (Dec. 22, 2005), *available at* http://www.usdoj.gov/ag/readingroom/surveillance6.pdf [hereinafter Moschella Letter] ("As described by the President, the NSA intercepts certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization.").

16. Gonzales/Hayden, *Press Briefing*, *supra* note 1 (Alberto Gonzales: "[W]e have to have a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda.").

17. *Id.*

18. Hayden, *Press Club*, *supra* note 1 ("We are going after very specific communications that our professional judgment tells us we have reason to believe are those associated with people who want to kill Americans.").

19. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the S. Comm. on the Judiciary*, 109th Cong. 42 (2006) [hereinafter *Hearings*] ("[I]nformation is collected, information is retained, and information is disseminated in a way to protect the privacy interests of all Americans.") (testimony of Alberto R. Gonzales, Att'y Gen. of the United States).

20. Gonzales/Hayden, *Press Briefing*, *supra* note 1 ("QUESTION: General, are you able to say how many Americans were caught in this surveillance? / ATTORNEY GENERAL GONZALES: I'm not—I can't get into the specific numbers because that information remains classified. Again, this is not a situation where—of domestic spying. To the extent that there is a moderate and heavy communication involving an American citizen, it would be a communication where the other end of the call is outside the United States and where we believe that either the American citizen or the person outside the United States is somehow affiliated with al Qaeda.").

21. *Id.* (Michael Hayden: "The period of time in which we do this is, in most cases, far less than that which would be gained by getting a court order."); *Hearings*, *supra* note 19, at 11 ("The program is triggered only when a career professional at the NSA has reasonable grounds to believe that one of the parties to a communication is a member or agent of al Qaeda or an affiliated terrorist organization." (testimony of Alberto R. Gonzales, Att'y Gen. of the United States)); Hayden, *Press Club*, *supra* note 1 ("QUESTION: . . . Just to clarify sort of what's been said, from what I've heard you say today and an earlier press conference, the change from going around the FISA law was to—one of them was to lower the standard from what they call for, which is basically probable cause to a reasonable basis; and then to take it away from a federal court judge, the FISA court judge, and hand it over to a shift supervisor at NSA. Is that what we're talking about here—just for clarification? / GEN. HAYDEN: You got most of it right. The people who make the judgment, and the one you just referred to, there are only a handful of people at NSA who can make that decision. They're all senior executives, they are all

nor the Attorney General authorized the specific interceptions.[22] Instead, an NSA "shift supervisor" was authorized to approve the selection of targets or of communications to be intercepted.[23]

Under the TSP, communications were intercepted without probable cause to believe that the surveillance targets had committed or were about to commit any crime. Rather, NSA intercepted communications when the agency had, in its own judgment, merely a "*reasonable basis to conclude* that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[24] Principal Deputy Director for National Intelligence (and former NSA Director) General Michael Hayden admitted that "[t]he trigger is quicker and a bit softer than it is for a FISA warrant,"[25] and suggested that the standard is "[i]nherent foreign intelligence value."[26] Attorney General Gonzales also conceded that the standard used is not criminal "probable cause."[27]

---

counterterrorism and al Qaeda experts. So I—even though I—you're actually quoting me back, Jim, saying, "shift supervisor." To be more precise in what you just described, the person who makes that decision, a very small handful, senior executive. So in military terms, a senior colonel or general officer equivalent; and in professional terms, the people who know more about this than anyone else. / QUESTION: Well, no, that wasn't the real question. The question I was asking, though, was since you lowered the standard, doesn't that decrease the protections of the U.S. citizens? And number two, if you could give us some idea of the genesis of this. Did you come up with the idea? Did somebody in the White House come up with the idea? Where did the idea originate from? Thank you. / GEN. HAYDEN: Let me just take the first one, Jim. And I'm not going to talk about the process by which the President arrived at his decision. I think you've accurately described the criteria under which this operates, and I think I at least tried to accurately describe a changed circumstance, threat to the nation, and why this approach—limited, focused—has been effective." Gonzales/Hayden, *Press Briefing*, *supra* note 1 ("[T]he Supreme Court has long held that there are exceptions to the warrant requirement in—when special needs outside the law enforcement arena. And we think that that standard has been met here." (statement of Alberto R. Gonzales, Att'y Gen. of United States)).

22. Hayden, *Press Club*, *supra* note 1 ("These are communications that we have reason to believe are al Qaeda communications, a judgment made by American intelligence professionals, not folks like me or political appointees . . . .").

23. Gonzales/Hayden, *Press Briefing*, *supra* note 1 (Michael Hayden: "The judgment [to target a communication] is made by the operational work force at the National Security Agency using the information available to them at the time, and the standard that they apply—and it's a two-person standard that must be signed off by a shift supervisor, and carefully recorded as to what created the operational imperative to cover any target, but particularly with regard to those inside the United States."); *see also Hearings*, *supra* note 19, at 34 (Alberto Gonzales: "The decisions as to which communications are to be surveilled are made by intelligence experts out at NSA.").

24. Gonzales/Hayden, *Press Briefing*, *supra* note 1 (statement of Alberto Gonzales) (emphasis added); *see also* Hayden, *Press Club*, *supra* note 1 (explaining that the NSA intercepts calls it has "a reasonable basis to believe" involves affiliates of al Qaeda).

25. *Id.*

26. *Id.* ("Inherent foreign intelligence value is one of the metrics we must use to ensure that we conform to the Fourth Amendment's reasonable standard when it comes to protecting the privacy of these kinds of people.").

27. *Hearings*, *supra* note 19, at 99–100 ("I think it is probable cause. But it is not probable

The TSP intercepted communications that were subject to the requirements of FISA.[28] FISA states that "[a] person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute."[29] The Attorney General admitted that the TSP constituted "electronic surveillance" as defined in and governed by FISA:

> Now, in terms of legal authorities, the Foreign Intelligence Surveillance Act provides—requires a court order before engaging in this kind of surveillance that I've just discussed and the President announced on Saturday, unless there is somehow—there is—unless otherwise authorized by statute or by Congress. That's what the law requires.[30]

Nonetheless, the TSP was used "in lieu of" the procedures specified under FISA.[31] In the words of General Michael Hayden, the Principal Deputy Director for National Intelligence, "this is a more . . . 'aggressive' program than would be traditionally available under FISA."[32]

---

cause as to guilt . . . or probable cause as to a crime being committed. It is probable cause that a party to the communication is a member or agent of al Qaeda. The precise language that I would like to refer to is a reasonable grounds to believe. Reasonable grounds to believe that a party to the communication is a member or agent of al Qaeda or of an affiliated terrorist organization. . . . It is a probable cause standard, in my judgment." (testimony of Alberto R. Gonzales, Att'y Gen. of the United States).

28. In *ACLU v. NSA*, Judge Batchelder argued that because the ACLU plaintiffs "have not shown, and cannot show, that the NSA engages in activities satisfying the statutory definition of 'electronic surveillance' [they] cannot demonstrate that FISA does apply." 493 F.3d 644, 683 (6th Cir. 2007), *cert. denied*, No. 07-468, 2008 WL 423556, at *1 (U.S. Feb. 19, 2008); *see also id.* at 681 ("These factors raise a host of intricate issues, such as whether the NSA's wiretapping actually involves 'electronic surveillance' as defined in FISA . . . ."). Judge Batchelder's argument is willfully blind to Attorney General Gonzales's admission dating back to December 2005 that the surveillance carried out by the program was subject to the strictures of FISA—in other words, that it constituted "electronic surveillance" under 50 U.S.C. § 1801(f). In any event, the claim that the program did not constitute "electronic surveillance' subject to FISA would be nonsensical in the face of the fact that the government subsequently went to the FISA Court for orders authorizing what had been done under the TSP, given that the FISA Court's jurisdiction extends only to authorizing electronic surveillance. *Cf. id.* at 713–17 (Gilman, J. dissenting).

29. 50 U.S.C. § 1809 (2000).

30. Gonzales/Hayden, *Press Briefing*, *supra* note 1 (statement of Alberto Gonzales).

31. *Id.* (statement of Michael Hayden); *see also* Hayden, *Press Club*, *supra* note 1 ("If FISA worked just as well, why wouldn't I use FISA? To save typing? No. There is an operational impact here, and I have two paths in front of me, both of them lawful, one FISA, one the presidential—the president's authorization. And we go down this path because our operational judgment is it is much more effective. So we do it for that reason."); Gonzales/Hayden, *Press Briefing*, *supra* note 1 (Michael Hayden: "What you're asking me is, can we do this program as efficiently using the one avenue provided to us by the FISA Act, as opposed to the avenue provided to us by subsequent legislation and the President's authorization. Our operational judgment, given the threat to the nation that the difference in the operational efficiencies between those two sets of authorities are such that we can provide greater protection for the nation operating under this authorization.").

32. Gonzales/Hayden, *Press Briefing*, *supra* note 1 (statement of Michael Hayden); *see also* Hayden, *Press Club*, *supra* note 1 ("In the instances where this program applies, FISA does not

The administration considered asking Congress to amend FISA to permit the NSA spying program. But it elected not to do so until August 2007 and instead originally ordered its implementation in secret. Attorney General Gonzales acknowledged that administration officials consulted various members of Congress about seeking legislation to authorize the TSP but initially chose not to do so because they were advised that it would be "difficult if not impossible" to obtain.[33]

Despite the government's argument that it could not conduct the electronic surveillance it needed to conduct within the limits of FISA, on January 10, 2007, the FISA Court

> issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the [parties to the communication] is a member or agent of al Qaeda or an associated terrorist organization.[34]

The government subsequently took the position that, because of the new "FISA Court orders, any electronic surveillance that [had been] occurring as part of the TSP [was then] being conducted subject to the approval of the FISA Court, and [that] the President ha[d] decided not to reauthorize the TSP."[35]

The government then argued that the legal challenges to the TSP were moot as a result of the FISA Court orders. The plaintiffs in the various cases argued that voluntary cessation of illegal activity in the face of a court challenge does not render the challenge moot.[36]

In the summer of 2007, the Bush administration changed its strategy once again and intensively lobbied Congress to amend FISA to permit warrantless electronic surveillance.[37] Congress acquiesced to the

---

give us the operational effect that the authorities that the president has given us give us."); Moschella Letter, *supra* note 15 ("[T]he President determined that it was necessary following September 11 to create an early warning detection system. FISA could not have provided the speed and agility required for the early warning detection system.").

33. Gonzales/Hayden, *Press Briefing*, *supra* note 1 (Alberto Gonzales: "We have had discussions with Congress in the past—certain members of Congress—as to whether or not FISA could be amended to allow us to adequately deal with this kind of threat, and we were advised that that would be difficult, if not impossible.").

34. Letter from Alberto R. Gonzales, Attorney Gen., to Patrick Leahy, Chairman, Senate Comm. on the Judiciary, & Arlen Specter, Ranking Minority Member, Senate Comm. on the Judiciary (Jan. 17, 2007) [hereinafter Gonzales Letter], *available at* http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf.

35. Defendants' Supplemental Memorandum in Support of Motion To Dismiss or for Summary Judgment in Center for Constitutional Rights v. Bush at 2, Ctr. for Constitutional Rights v. Bush, No. M:06-cv-01791-VRW (N.D. Cal. filed Jan. 17, 2006); *see also* Brief for the United States at 9–10, Hepting v. AT&T Corp., 508 F.3d 898 (9th Cir. 2007) (No. 06-17137).

36. *See infra* Part IV, discussing whether the legal challenges were rendered moot.

37. *See* Letter from J.M. McConnell, Dir. of Nat'l Intelligence, to Harry Reid, Majority Leader, U.S. Senate, et al. (July 27, 2007) (on file with the University of Miami Law Review).

administration and in August enacted amendments that permitted the warrantless electronic surveillance of any person reasonably believed to be outside of the United States.[38] Presumably, any foreign-intelligence electronic surveillance that is taking place at the time of this writing is being conducted under the 2007 amendments to FISA.

III. THE TERRORIST SURVEILLANCE PROGRAM WAS UNCONSTITUTIONAL

A. *The Statutory Scheme Regulating Foreign Intelligence Surveillance Before the Legislation Enacted in August 2007*

FISA regulates electronic surveillance for foreign-intelligence and national-security purposes within the United States.[39] Congress enacted FISA in 1978 after revelations of widespread spying on Americans by federal law-enforcement and intelligence agencies—including NSA.[40] The Senate Judiciary Committee stated that the legislation was "in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."[41] FISA was intended to strike a careful balance between protecting civil liberties and preserving the "vitally important government purpose" of obtaining valuable intelligence in order to safeguard national security.[42]

With minor exceptions, FISA authorized "electronic surveillance"

---

38. *See infra* Part V for a discussion of the amendments and the constitutionality of the new statutory framework.

39. 50 U.S.C. §§ 1801–1862 (2000).

40. A special congressional committee known as the Church Committee (after its Chairman, Sen. Frank Church) concluded, after lengthy investigation and hearings:

> The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials.

S. Rep. No. 95-604, at 8 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3909.

The Church Committee noted that Congress had "a particular obligation to examine the NSA, in light of its tremendous potential for abuse." *The National Security Agency and Fourth Amendment Rights: Hearings Before the S. Select Comm. To Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 2 (1975), *available at* http://cryptome.org/nsa-4th.htm (statement of Sen. Church, Chairman, S. Select Comm. To Study Governmental Operations with Respect to Intelligence Activities). In its final report, the Church Committee warned that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature." S. Rep. No. 94-755, at 1 (1976).

41. S. Rep. No. 95-604, at 7 (1977), *as reprinted* in 1978 U.S.C.C.A.N. 3904, 3908.

42. *Id.* at 9, 1978 U.S.C.C.A.N. at 3910.

for foreign-intelligence purposes only on certain specified showings and only if approved by the FISA Court, which the legislation established. FISA governs only statutorily defined "electronic surveillance," principally surveillance targeted at U.S. citizens or permanent residents within the United States or electronic surveillance gathered within the United States.[43] Accordingly, as originally enacted, FISA left ungoverned interceptions made abroad of a foreign target's electronic communications. Electronic surveillance, as originally governed by FISA, was permissible on a court order, which had to be based on a showing of probable cause that the target of the surveillance is a "foreign power" or an "agent of a foreign power." This would include a member of any "group engaged in international terrorism."[44] FISA does not require

---

43. Before the 2007 amendments, FISA defined "electronic surveillance" in 50 U.S.C. § 1801(f) to include:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (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 the consent of any party thereto, if such acquisition occurs in the United States;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; 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, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

44. 50 U.S.C. § 1801(a) and (b) define foreign powers and agents of foreign powers:

> (a) "Foreign power" means—
>
> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons; or
>
> (6) an entity that is directed and controlled by a foreign government or governments.
>
> (b) "Agent of a foreign power" means—

probable cause of criminal activity to justify electronic surveillance.

Congress sought to make clear that electronic surveillance was to be undertaken only under federal statute. To that end, Congress expressly provided that FISA and specified provisions of the federal criminal code (which govern wiretaps for criminal investigations) are the "*exclusive* means by which electronic surveillance . . . may be conducted."[45] To underscore the point, Congress made it a crime, under two separate provisions of the U.S. Code, to undertake electronic surveillance not authorized by statute. FISA itself made it a crime to conduct "electronic surveillance under color of law except as authorized by statute."[46] Title 18 is even more explicit: 18 U.S.C. § 2511 makes it a crime to conduct wiretapping except as "specifically provided in this chapter," § 2511(1), or as authorized by FISA.

Signing FISA into law, President Carter acknowledged that it applied to *all* electronic surveillance, stating:

> The bill requires, for the first time, a prior judicial warrant for *all* electronic surveillance for foreign intelligence or counterintelligence purposes in the United States in which communications of U.S. persons might be intercepted. It clarifies the Executive's authority to gather foreign intelligence by electronic surveillance in the

---

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(C) engages in international terrorism or activities in preparation therefore; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

45. 18 U.S.C. § 2511(2)(f) (emphasis added).

46. 50 U.S.C. § 1809(a)(1).

United States.[47]

In subjecting foreign-intelligence electronic surveillance to strict statutory limits, FISA marked a substantial change in the law. Before FISA's enactment, Congress had chosen not to regulate foreign-intelligence surveillance. In fact, when Congress regulated criminal wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, it expressly recognized that it was leaving unregulated foreign-intelligence surveillance:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) 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 other hostile acts of a foreign power, *to obtain foreign intelligence information deemed essential to the security of the United States*, or to protect national security information against foreign intelligence activities.[48]

When Congress enacted FISA, however, it repealed the above provision, and substituted the language quoted above providing that FISA and Title III were the "exclusive means" for engaging in electronic surveillance and that any such surveillance conducted outside the authority of those statutes was not only prohibited, but a crime.

Congress specifically addressed in FISA the question of domestic wiretapping during wartime. In 18 U.S.C. § 1811, entitled "Authorization during time of war," FISA dictated that "[n]otwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information *for a period not to exceed fifteen calendar days following a declaration of war by the Congress.*"[49] Thus, even when Congress declares war, the law limited warrantless wiretapping to the first fifteen days of the conflict. The legislative history of this provision explains that if the President needed further surveillance powers because of the special nature of the particular war at hand, fifteen days would be sufficient for Congress to consider and enact further statutory authorization.[50]

Congress also anticipated that emergencies might require the gov-

47. Statement on Signing the Foreign Intelligence Surveillance Act of 1978, 2 PUB. PAPERS 1853 (Oct. 25, 1978).

48. Pub. L. No. 90-351, § 2511(3), 82 Stat. 197 (emphasis added).

49. 50 U.S.C. § 1811 (emphasis added).

50. "The Conferees intend that this [15-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency. . . . The conferees expect that such amendment would be reported with recommendations within 7 days and that each House would vote on the amendment within 7 days thereafter." H.R. REP. No. 95-1720, at 34 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4063, 4048.

ernment to initiate electronic surveillance before a warrant can be obtained. The original legislation allowed the government to intercept conversations without a warrant for twenty-four hours while it sought a warrant from the court. In December 2001 Congress subsequently amended FISA to extend that time period from twenty-four to seventy-two hours with this emergency-warrant provision.[51]

B. *The Terrorist Surveillance Program and the Constitutional Powers of the President*[52]

Both FISA and 18 U.S.C. § 2511 specify that foreign-intelligence electronic surveillance must be conducted under statute and court order. Despite the specific legislation directly on point, President Bush declined to ask Congress to amend FISA to permit the TSP to go forward. He did seek other amendments to FISA in the immediate aftermath of the terrorist attacks of September 11 in what ultimately became the USA PATRIOT Act.[53] On its face, because the TSP conducted "electronic surveillance" outside of the process carefully prescribed by FISA, it would seem evident that the TSP violated FISA and 18 U.S.C. § 2511, and that it was contrary to law.[54]

The government argued that the TSP was legal and constitutional for two reasons. First, it submitted that the President has inherent constitutional authority to engage in warrantless electronic surveillance of foreign targets that are national-security threats, whether or not Congress has authorized such surveillance. Second, the government argued that Congress had in fact authorized the surveillance by passing the AUMF after September 11. Neither argument is persuasive.

---

51. 50 U.S.C. § 1805(f), *amended by* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314 (a)(2)(B), 115 Stat. 1394, 1402 (2001).

52. The TSP was also subject to attack on the ground that it violated the Fourth Amendment for the President to engage in warrantless electronic surveillance, regardless of whether Congress had authorized it. *See* discussion *infra* Part V detailing Fourth Amendment argument.

53. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of U.S.C.).

54. The Congressional Research Service independently found that the NSA program violates federal law. *See* Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Attorneys, Am. Law Div., Cong. Research Serv., Presidential Authority To Conduct Warrantless Electronic Surveillance To Gather Foreign Intelligence Information (Jan. 5, 2006), *available at* http://www.fas.org/sgp/crs/intel/m010506.pdf. To the extent that the NSA spying program violated federal law and the Constitution, and was therefore "contrary to law," it could be argued that it gave rise to injunctive relief under the Administrative Procedure Act. *See* 5 U.S.C. § 706(2) (2000) (stating that a reviewing court shall "hold unlawful and set aside agency action" that is "otherwise not in accordance with law," and that is taken "in excess of statutory jurisdiction, authority, or limitations").

C. *Whether the President Has Inherent Constitutional Authority To Conduct Warrantless Electronic Surveillance*

The TSP violated basic principles of the separation of powers. Wiretapping Americans, even during wartime, is not an exclusive executive prerogative immune from regulation by the other branches. Through FISA, foreign-intelligence wiretapping has been subject to legislative and judicial checks for nearly thirty years, and its constitutionality in so restricting the Executive has not previously been challenged.

Analysis of the separation-of-powers question presented by the NSA spying program is governed by *Youngstown Sheet & Tube Co. v. Sawyer* and particularly by Justice Jackson's influential concurring opinion in it.[55] In that case, the Supreme Court held that President Truman had no implied constitutional power as commander in chief to seize American steel companies to assure the production of materials necessary to prosecute the Korean War. In his concurring opinion, Justice Jackson analyzed three different situations in which the President might attempt to exercise implied power under the Constitution: (1) Presidential action under an express or implied authorization by Congress, in which case Presidential authority is at is maximum; (2) Presidential action in the face of Congressional silence, which Justice Jackson characterized as a "zone of twilight"; and (3) Presidential action contrary to the expressed or implied will of Congress, in which case Presidential power is at "its lowest ebb."[56]

The TSP falls within Justice Jackson's third category, because FISA expressly required individualized judicial approval of foreign-intelligence-electronic surveillance of the type involved in the TSP and made it a crime to engage in electronic surveillance without statutory authority. Because the President acted in contravention of FISA's express limits, his constitutional power is at its "lowest ebb," and he may act in contravention of statute only if Congress may be "disabl[ed] . . . from acting upon the subject"[57] of foreign-intelligence electronic surveillance within the United States. In fact, Congress acted well within its Article I powers in regulating executive intrusions on the privacy of U.S. persons in international-electronic communications and did not intrude on the President's Article II role.

There is no doubt that Presidents have routinely collected signals intelligence on the enemy during wartime. Indeed, for most of our history Congress did not regulate foreign intelligence gathering in any way. But as Justice Jackson made clear in *Youngstown*, to say that a President

55. 343 U.S. 579 (1952).
56. *Id.* at 635–38 (Jackson, J., concurring).
57. *Id.* at 637–38.

may undertake certain conduct in the absence of contrary congressional action does not mean that he may undertake that action where Congress has addressed the issue and disapproved of the action.[58] Here, Congress has not only disapproved of the action the President has taken, but it has made it a crime.

The remaining question, then, is whether Congress is disabled from acting on the subject. The administration has argued that the President has exclusive constitutional authority over "the means and methods of engaging the enemy[,]"[59] and that FISA, therefore, is unconstitutional if it prohibits warrantless "electronic surveillance" deemed necessary by the President in the conflict with al Qaeda.[60] The Justice Department has also argued that even if Congress may regulate "signals intelligence" during wartime to some degree, FISA impermissibly intrudes on the President's exercise of his commander in chief role if it precludes warrantless wiretapping of Americans in the context of the NSA spying program.[61] Case law and historical precedent directly contradict the argument that conduct undertaken by the commander in chief that has some relevance to "engaging the enemy" is immune from congressional regulation. Every time the Supreme Court has confronted a statute limiting the commander in chief's authority, it has upheld the statute. No precedent holds that the President, when acting as commander in chief, is free to disregard an act of Congress designed specifically to restrain the President.

There can be no serious dispute that Congress's Article I powers afford it the authority to regulate wiretapping of U.S. persons on American soil. Further, the Supreme Court in *United States v. United States District Court (Keith)*, expressly held that Congress had the power to set forth reasonable standards governing the warrant process for domestic national-security surveillance:

> We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. 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

58. *See id.* at 635–38.

59. U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 32 n.15 (Jan. 19, 2006) [hereinafter DOJ Memo], *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

60. *Id.* at 29–35.

61. *Id.*

prescribe.[62]

As Congress properly recognized in enacting FISA,[63] "even if the President has the inherent authority in the absence of legislation to authorize warrantless electronic surveillance for foreign intelligence purposes, Congress . . . [can] regulate the conduct of such surveillance by legislating a reasonable procedure, which then becomes the exclusive means by which such surveillance may be conducted."[64] This analysis was "supported by two successive Attorneys General."[65]

---

62. 407 U.S. 297, 323–24 (1972).

63. Indeed, Congress modeled FISA along lines suggested by the Supreme Court in *Keith*:

> Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. . . . [T]he warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection . . . .
>
> . . . .
>
> It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (*e.g.*, the District Court for the District of Columbia or the Court of Appeals for the District of Columbia Circuit); and that the time and reporting requirements need not be so strict as those in § 2518.

Id. at 322–23.

64. H.R. REP. No. 95-1283, pt. 1, at 24 (1978).

65. *Id.*; *see also Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 31 (1978) (letter from John M. Harmon, Assistant Att'y Gen., Office of Legal Counsel, to Edward P. Boland, Chairman, H. Permanent Select Comm. on Intelligence) ("[I]t seems unreasonable to conclude that Congress, in the exercise of its powers in this area, may not vest in the courts the authority to approve intelligence surveillance."). Attorney General Griffin Bell supported FISA in part because "no matter how well intentioned or ingenious the persons in the Executive branch who formulate these measures, the crucible of the legislative process will ensure that the procedures will be affirmed by that branch of government which is more directly responsible to the electorate." *Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence*, 95th Cong. 12 (1978); S. REP. No. 95-604, at 16 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3917 ("The basis for this legislation—concurred in by the Attorney General—that even if the President has an 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.").

President Ford's Attorney General Edward Levi, testifying before a Senate Judiciary subcommittee in support of FISA, stated:

> I really cannot imagine a President, if this legislation is in effect, going outside the legislation for matters which are within the scope of this legislation. . . . I really do not think its is quite appropriate to describe the Presidential authority as either being absolute on the one hand, or nonexistent on the other. . . . [T]here is a middle category where, assuming Presidential authority, that authority nevertheless, can be directed by the Congress.

In fact, FISA establishes a reasonable procedure and expressly permits wiretapping of foreign agents, including members of international terrorist organizations and merely requires judicial confirmation that there is a factual basis for doing so. First, FISA is triggered only when surveillance is targeting a "United States person who is in the United States," or the surveillance "acquisition occurs in the United States."[66] FISA does not regulate electronic surveillance acquired abroad and targeted at non-U.S. persons. Thus, it does not limit in any respect wholly foreign surveillance of al Qaeda, or indeed even of all persons in Afghanistan.

Second, even when the target of surveillance is a U.S. person within the United States, or the information is physically acquired within the United States, FISA permits wiretaps approved by the FISA Court based on a showing of probable cause that the target is an "agent of a foreign power," which includes a member of a terrorist organization.[67]

Because FISA leaves unregulated electronic surveillance conducted outside the United States and not targeted at U.S. persons, it leaves to the President's unfettered discretion a wide swath of "signals intelligence." Moreover, FISA does not actually prohibit *any* signals intelligence regarding al Qaeda, but merely requires judicial approval where the surveillance targets a U.S. person or is acquired here. As such, the statute cannot reasonably be said to intrude impermissibly on the President's ability to "engage the enemy," and certainly does not come anywhere close to "prohibit[ing] the President from undertaking actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack[,]" as the Justice Department has asserted.[68]

The President's broad assertion of unchecked authority to choose the "means and methods of engaging the enemy" finds no support in the text of the Constitution or the history of executive-legislative interactions during wartime. Every time the Supreme Court has addressed the propriety of executive action contrary to congressional statute during wartime, it has required the President to adhere to legislative limits on his authority.[69] In *Youngstown*, as noted above, the Court invalidated President Truman's wartime seizure of the steel mills, where Congress

---

Foreign Intelligence Surveillance Act of 1976: Hearing on S. 743, S. 1888, and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary, 94th Cong. 16 (1976).

66. 50 U.S.C. § 1801(f)(1)–(2) (2000).

67. *See id.* §§ 1801 (a)–(b), 1805(a)–(b). If the target is not a U.S. person, it is sufficient to show that he is a "lone wolf" terrorist. *See id.* § 1801(b)(1).

68. DOJ Memo, *supra* note 59, at 35 (emphasis omitted).

69. *See, e.g.*, Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952); Little v. Barreme, 6 U.S. (2 Cranch) 170 (1804).

had "rejected an amendment which would have authorized such governmental seizures in cases of emergency."[70]

In *Little v. Barreme*, the Court held unlawful a seizure pursuant to presidential order of a ship during the "Quasi War" with France.[71] The Court found that Congress had authorized the seizure only of ships going *to* France, and therefore the President could not unilaterally order the seizure of a ship coming *from* France.[72] Just as in *Youngstown,* the Court invalidated executive action taken during wartime, said to be necessary to the war effort, but implicitly disapproved by Congress.[73]

President Bush's unilateral executive action with respect to NSA is more sharply in conflict with congressional legislation than the presidential actions in either *Youngstown* or *Barreme*. In those cases, Congress had merely failed to give the President the authority in question, and thus the statutory limitation was *implicit*. Here, Congress went further and *expressly prohibited* the President from taking the action in question. And it did so in the strongest way possible, by making the conduct a crime.

More recent Supreme Court decisions, in the context of the current conflict with al Qaeda, reaffirm the teachings of *Youngstown* and *Barreme*. In *Rasul v. Bush*,[74] the administration maintained that it would be unconstitutional to interpret the habeas-corpus statute to afford judicial review to enemy combatants held at Guantánamo Bay because it "would directly interfere with the Executive's conduct of the military campaign against al Qaeda and its supporters,"[75] and would raise "grave constitutional problems."[76] The six-justice majority refused to accept this argument, and held that Congress had conferred habeas jurisdiction on the federal courts to entertain the detainees' habeas actions.[77] Justice Scalia, writing for the three dissenters, agreed that Congress *could have* extended habeas jurisdiction to the Guantánamo detainees, and differed

70. *Youngstown*, 343 U.S. at 586.

71. 6 U.S. (2 Cranch) at 178.

72. *Id.* at 176–78.

73. Similarly, in *Ex parte Milligan*, the Court unanimously held that the Executive violated the Habeas Corpus Act by failing to discharge from military custody a petitioner held by order of the President and charged with, inter alia, affording aid and comfort to rebels, inciting insurrection, and violation of the laws of war. 71 U.S. (4 Wall.) 2, 115–17, 131 (1866); *see also Ex parte* Endo, 323 U.S. 283 (1944) (finding that President had no authority to detain loyal U.S. citizen during war where Congress had not authorized it); *Milligan*, 71 U.S. (4 Wall.) at 133 (Chase, C.J., concurring) ("The constitutionality of this act has not been questioned and is not doubted. . . . [But the act] limited this authority [of the President to suspend habeas] in important respects.").

74. 542 U.S. 466 (2004).

75. Brief for the Respondents at 42, Rasul v. Bush, 542 U.S. 466 (2004) (No. 03-334).

76. *Id.* at 44.

77. *See Rasul*, 542 U.S. at 485.

only about whether Congress had in fact done so.[78] Thus, not a single Justice accepted the Bush administration's contention that the President's role as commander in chief may not be limited by congressional and judicial oversight.

Similarly, in *Hamdi v. Rumsfeld*,[79] the Court rejected the President's argument that courts may not inquire into the factual basis for the detention of a U.S. citizen as an enemy combatant.[80] As Justice O'Connor wrote for the plurality, "[w]hatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake."[81]

Detaining enemy combatants captured on the battlefield is surely closer to the core of "engaging the enemy" than is warrantless wiretapping of U.S. persons within the United States. Yet the Supreme Court in the enemy-combatant cases squarely held that both Congress and the courts had a proper role to play in reviewing and restricting the President's detention power. These cases thus refute the administration's contention that Congress may not enact statutes that regulate and limit the President's choices of the "means and methods of engaging the enemy" as commander in chief.

The Constitution's text confirms this conclusion. The Framers of the Constitution made the President the commander in chief, but otherwise assigned substantial power to Congress in connection with war making. Article I gives Congress the power to declare war and to authorize more limited forms of military enterprises (through "Letters of Marque and Reprisal");[82] to raise and support the army and navy;[83] to prescribe "Rules for the Government and Regulation of the land and naval Forces;"[84] to define "Offenses against the Law of Nations;"[85] and to spend federal dollars.[86] In addition, Congress has expansive authority "[t]o make all Laws which shall be necessary and proper for carrying into Execution . . . all . . . Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof."[87] The President, meanwhile, is constitutionally obligated to

78. *Id.* at 506 (Scalia, J., dissenting).
79. 542 U.S. 507 (2004).
80. *See id.* at 533 (plurality opinion).
81. *Id.* at 536 (citing Mistretta v. United States, 488 U.S. 361 (1989)).
82. U.S. CONST. art. I, § 8, cl. 11.
83. *Id.* cls. 12–13.
84. *Id.* cl. 14
85. *Id.* cl. 10.
86. *Id.* cl. 1.
87. *Id.* cl. 18.

"take Care that the Laws be faithfully executed,"[88] which, of course, would include FISA. The commander in chief's role is not even described as a "power," and is plainly subject to the legislative powers assigned to Congress by Article I. These constitutional provisions make clear that although the Framers recognized the necessity and desirability of giving the President the authority to direct the troops, the Framers also recognized the real dangers of Presidential wartime authority—and sought very explicitly to limit that authority by vesting in Congress broad authority to create, fund, and regulate the very forces that engage the enemy. These textual provisions cannot be read to afford the President unchecked authority to choose the "means and methods of engaging the enemy."

History also supports this conclusion. Congress has routinely enacted statutes regulating the commander in chief's "means and methods of engaging the enemy." It has subjected the Armed Forces to the Uniform Code of Military Justice, which expressly restricts the means the President may employ in "engaging the enemy."[89] It has enacted statutes setting forth the rules for governing occupied territory, and these statutes displace presidential regulations governing such "enemy territory" in the absence of legislation.[90] And most recently, it has enacted statutes prohibiting torture under all circumstances,[91] and prohibiting the use of inhuman, cruel, and degrading treatment by U.S. officials and military personnel anywhere in the world.[92]

If the Bush administration were correct that Congress cannot interfere with the commander in chief's discretion in "engaging the enemy," all of these statutes would be unconstitutional. Torturing a suspect, no less than wiretapping an American, might provide information about the enemy that could conceivably help prevent a future attack, yet President Bush has conceded that Congress can prohibit that conduct.[93] Congress has as much authority to regulate wiretapping of Americans as it has to regulate torture and inhuman treatment of foreign detainees.[94] Accord-

88. *Id.* art. II, § 3.

89. 10 U.S.C. §§ 801–946 (2000).

90. *See* Santiago v. Nogueras, 214 U.S. 260, 265–66 (1909).

91. 18 U.S.C. §§ 2340–2340A.

92. Detainee Treatment Act of 2005, Pub. L. No. 109-148, § 1003, 119 Stat. 2739, 2739–40 (2005) (to be codified at 42 U.S.C. § 2000dd).

93. In an interview on CBS News, President Bush said, "I don't think a President can order torture, for example. . . . There are clear red lines." Eric Lichtblau & Adam Liptak, *Bush and His Senior Aides Press On in Legal Defense for Wiretapping Program*, N.Y. TIMES, Jan. 28, 2006, at A13.

94. The DOJ Memo oddly suggested that Congress's authority to enact FISA is less clear than was the power of Congress to act in *Youngstown* and *Little v. Barreme*, both of which involved congressional action at what the DOJ calls the "core" of Congress's enumerated Article I powers—regulating commerce. DOJ Memo, *supra* note 59, at 32–34. But FISA was also enacted

ingly, the President cannot simply contravene Congress's clear criminal prohibitions on electronic surveillance.

In support of its argument that the President's actions were constitutional, the Justice Department relied on a FISA Court decision and a series of lower federal-court cases that addressed the issue of the President's power. In *In re Sealed Case*, the FISA Court did assume, in dictum, that the President has some inherent authority to gather foreign intelligence, and that Congress cannot "encroach on the President's constitutional power."[95] But the court plainly did not mean that *any regulation* of foreign intelligence gathering amounts to impermissible "encroachment," because it upheld FISA in that very case (as has every court to consider it since its enactment in 1978). Indeed, the court did not even attempt to define what sorts of regulations would constitute impermissible "encroachment."

All of the lower federal-court cases that have recognized inherent presidential authority to conduct foreign-intelligence surveillance addressed the President's pre-FISA authority. The President's authority before FISA was enacted differed radically from his authority after FISA. Before FISA was enacted, Congress had left open the question whether the President has "constitutional power . . . to obtain foreign intelligence information deemed essential to the security of the United States."[96] Before FISA, the President was acting "in the absence of either a Congressional grant or denial of authority" and acting in Justice Jackson's "category two," the "zone of twilight" in which the President and Congress "may have concurrent authority, or in which [the] distribution [of power] is uncertain."[97]

But when Congress enacted FISA in the wake of demonstrated abuses of that power, it repealed the provision approving of inherent-presidential foreign-intelligence gathering, and made it a crime to conduct wiretapping without congressional authority. In authorizing NSA to conduct warrantless wiretapping in contravention of FISA's criminal

---

under "core" Article I powers—including the same foreign-commerce power at issue in *Little*, and, as applied to NSA, Congress's powers under the Rules for the Government and Regulation of the Land and Naval Forces, and the Necessary and Proper Clauses.

95. 310 F.3d 717, 742 (FISA Ct. Rev. 2002) (per curiam).

96. 18 U.S.C. § 2511(3) (1970) (repealed 1978). The Government argued in *Keith* that this provision in Title III amounted to recognition by Congress that the President had authority to conduct electronic surveillance in national-security cases without judicial approval. The Supreme Court flatly rejected this contention and concluded that the section conferred no power on the President, but merely meant that Congress was not legislating in Title III with respect to national-security surveillances. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 303–06, 308 (1972). The Court held that Title III left the President only with such power as the Constitution might confer with respect to national-security surveillance and neither expanded nor contracted such power. *Id.* at 308.

97. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (Jackson, J. concurring).

prohibition, the President is therefore acting in Justice Jackson's "category three." There, the President's power is at its "lowest ebb." Thus, that some lower federal courts may have ruled that the President may have had the power to act when Congress had been silent with respect to his power does not mean that the President can choose to violate a duly enacted criminal prohibition after Congress has "acted upon the subject."[98]

The authority on which the government relies to establish the President's constitutional authority is unconvincing. *United States v. Clay*,[99] *United States v. Brown*,[100] and *United States v. Butenko*,[101] were decided before FISA was enacted, which severely undercuts their precedential authority. The analysis in these cases is exceedingly brief, shallow, and unpersuasive.[102] *United States v. Truong Dinh Hung*,[103] although decided after FISA, involved surveillance that ended well before FISA was passed,[104] and conducts such an abbreviated analysis that it mentions the new statute only in a footnote and contains no analysis of FISA's impact on the President's implied authority under Justice Jackson's concurrence in *Youngstown*.[105] Judge Skelly Wright conducted a far more thorough, historical, and scholarly analysis in *Zweibon v. Mitchell*, in the plurality opinion that concluded that the President lacks constitutional power to conduct warrantless electronic surveillance.[106] That argument has been considerably strengthened by the passage of FISA, which demonstrated that Congress not only does not recognize any such general power on the part of the President but has made its attempted exercise a criminal offense.

Cases that establish the proposition that the President has preeminent authority with respect to the conduct of foreign affairs, such as *United States v. Curtiss-Wright Export Corp.*,[107] and *Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.*,[108] do not resolve the

98. *Cf. id.* at 638–39 (stating that the President could not ignore Congress's method of seizing steel mills).

99. 430 F.2d 165 (5th Cir. 1970), *rev'd*, 403 U.S. 698 (1971).

100. 484 F.2d 418 (5th Cir. 1973).

101. 494 F.2d 593 (3d Cir. 1974).

102. For a detailed analysis of the weaknesses of these opinions, see *Zweibon v. Mitchell*, 516 F.2d 594, 637–41 (D.C. Cir. 1975).

103. 629 F.2d 908 (4th Cir. 1980).

104. The surveillance at issue in *Truong* terminated in January 1978. *Id.* at 912 ("Truong's phone was tapped and his apartment was bugged from May, 1977 to January, 1978. . . . Truong and Humphrey were arrested on January 31, 1978."). FISA was enacted in October of that year. The court's holding therefore can relate only to the pre-FISA regime.

105. *See id.* at 914 n.4.

106. 516 F.2d at 614.

107. 299 U.S. 304, 319 (1936).

108. 333 U.S. 103, 109 (1948).

question whether the President has the specific power to conduct warrantless electronic surveillance.[109] Both of those cases involved presidential power exercised pursuant to congressional authorization. Moreover, the President's powers as commander in chief do not imply unilateral control over domestic policies, even those related to the conduct of foreign wars. As Justice Jackson warned in *Youngstown Sheet & Tube Co. v. Sawyer*:

> [N]o doctrine that the Court could promulgate would seem to me more sinister and alarming than that a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture. [110]

Indeed, Jackson explained that an argument that the commander in chief can act in the domestic sphere without restraint by the other branches stands the constitutional design on its head:

> The purpose of lodging dual titles in one man was to insure that the civilian would control the military, not to enable the military to subordinate the presidential office. No penance would ever expiate the sin against free government of holding that a President can escape control of executive powers by law through assuming his military role.[111]

D. *The Authorization To Use Military Force as a Potential Source of Congressional Authority*

The government argued that Congress authorized the NSA spying program when, on September 18, 2001, it enacted the AUMF against the perpetrators of the attacks on September 11 and those who harbor them.[112] The administration's argument was subject to three objections:

---

109. In *Zweibon v. Mitchell*, Judge Skelly Wright noted that the recognition of the President's implied powers in the area of foreign affairs "is inapposite to the question of how those powers are to be reconciled with the mandate of the Fourth Amendment." 516 F.2d at 621.

110. 343 U.S. 579, 642 (1952) (concurring opinion).

111. *Id.* at 646. Some statutes might impermissibly interfere with the President's role as commander in chief. If Congress sought to place authority to direct battlefield operations in an officer not subject to the President's supervision, for example, such a statute might well violate the President's role as commander in chief. Similarly, Congress should not be constitutionally permitted to micromanage tactical decisions in particular battles. But short of such highly unlikely hypotheticals, Congress has broad leeway to govern and regulate the armed services, to define the scope of a military conflict, to fund only the weapons and programs it approves, and certainly to protect the privacy expectations of Americans using telephone and e-mail communications.

112. Authorization for the Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (2001) (codified as amended at 50 U.S.C. § 1541). The Department of Justice set forth in detail its defense of the NSA program in DOJ Memo, *supra* note 59.

(1) it is directly contradicted by specific language in other federal statutes establishing that FISA and the criminal code are the "exclusive means" for conducting electronic surveillance; (2) it would require a repeal by implication of those statutes, and there is no basis in this situation for overcoming the strong presumption against implied repeals; and (3) it conflicts with the administration's claim that it chose not to ask Congress to amend FISA to authorize the program because several members of Congress told them that it would be "difficult, if not impossible," to obtain.

In FISA, Congress directly and specifically regulated domestic warrantless wiretapping for foreign-intelligence and national-security purposes, including during wartime. The administration's argument that the AUMF somehow trumped FISA would require the Court to override FISA's express and specific language based on an unstated general "implication" from the AUMF. This runs counter to the well-accepted rule that specific and "carefully drawn" statutes prevail over general statutes where there is a conflict.[113]

In light of Congress's specific regulation of electronic surveillance in FISA, and in particular its proviso that even a declaration of war authorizes no more than fifteen days of warrantless wiretapping,[114] there is no basis for finding in the AUMF's general language implicit authority for unchecked warrantless-domestic wiretapping. Neither the text of the AUMF nor its legislative history mentions authorizing surveillance, much less warrantless surveillance of conversations to which one party is an U.S. person within the United States. Indeed, in rejecting a similar argument by President Truman when he sought to defend the seizure of the steel mills during the Korean War on the basis of implied congressional authorization, Justice Frankfurter stated:

> It is one thing to draw an intention of Congress from general language and to say that Congress would have explicitly written what is inferred, where Congress has not addressed itself to a specific situation. It is quite impossible, however, when Congress did specifically address itself to a problem, as Congress did to that of seizure, to find secreted in the interstices of legislation the very grant of power which Congress consciously withheld. To find authority so explicitly withheld is not merely to disregard in a particular instance the clear will of Congress. It is to disrespect the whole legislative process and the constitutional division of authority between President and Congress.[115]

---

113. *See* Morales v. Trans World Airlines, Inc., 504 U.S. 374, 384 (1992) ([I]t is a commonplace of statutory construction that the specific governs the general . . . .").

114. 50 U.S.C. § 1811 (2000).

115. *Youngstown*, 343 U.S. at 609 (Frankfurter, J., concurring).

The administration relied on *Hamdi v. Rumsfeld*,[116] to argue that, just as the Supreme Court in that case construed the AUMF to provide sufficient statutory authorization for detention of American citizens captured on the battlefield in Afghanistan, the AUMF may also be read to authorize the President to conduct "signals intelligence" on the enemy, even if that includes electronic surveillance targeting U.S. persons within the United States.[117] Warrantless wiretapping of Americans at home, however, is far less clearly within the ambit of implied war powers than the power to detain an enemy soldier on a foreign battlefield.[118] Moreover, FISA specifically addresses wiretapping authority during wartime.[119]

The administration's AUMF argument cannot survive the decision of the Supreme Court in *Hamdan v. Rumsfeld*.[120] One of the many questions at issue in *Hamdan* was whether the AUMF provided congressional sanction for the military commissions instituted at Guantánamo

116. 542 U.S. 507 (2004).

117. DOJ Memo, *supra* note 59, at 2.

118. The Department of Justice argued that signals intelligence, like detention, is a "fundamental incident[ ] of waging war" and therefore is authorized by the AUMF. *Id.* at 13 (quoting *Hamdi*, 542 U.S. at 519) (internal quotation marks omitted). But what is properly considered an implied incident of conducting war is affected by the statutory landscape that exists at the time the war is authorized. Thus, even if warrantless electronic surveillance *of Americans* for foreign-intelligence purposes were a traditional incident of war when that subject was unregulated by Congress—which is far from obvious, at least in cases where the Americans targeted are not themselves suspected of being foreign agents or in league with terrorists—it can no longer be an implied incident after the enactment of FISA, which expressly addresses the situation of war and precludes such conduct beyond the first fifteen days of the conflict.

119. The administration argued that the AUMF might convey more authority than a declaration of war, noting that a declaration of war is generally only a single sentence. *Id.* at 26–27. But in fact, *every* declaration of war has been accompanied, *in the same enactment*, by an authorization to use military force. *See* Act of June 18, 1812, ch. 102, 2 Stat. 755 (declaring war against the United Kingdom in the War of 1812); Act of May 13, 1846, ch. 16, 9 Stat. 9 (declaring war against Mexico in the Mexican American War); Act of Apr. 25, 1898, ch. 189, 30 Stat. 364, 364 (declaring war against Spain in the Spanish American War); Joint Resolution of Apr. 6, 1917, ch.1, 40 Stat. 1, 1 (declaring war against Germany in World War I); Joint Resolution of Dec. 7, 1917, ch. 1, 40 Stat. 429 (declaring war against Austro-Hungarian Empire in World War I); Joint Resolution of Dec. 8, 1941, ch. 561, 55 Stat. 795 (declaring war against Japan in World War II); Joint Resolution of Dec. 11, 1941, ch. 564, 55 Stat. 796 (declaring war against Germany in World War II); Joint Resolution of Dec. 11, 1941, ch. 565, 55 Stat. 797 (declaring war against Italy in World War II); Joint Resolution of June 5, 1942, ch. 323, 56 Stat. 307(declaring war against Bulgaria in World War II); Joint Resolution of June 5, 1942, ch. 324, 56 Stat. 307 (declaring war against Hungary in World War II); Joint Resolution of June 5, 1942, ch. 325, 56 Stat. 307 (declaring war against Romania in World War II). It would be senseless to declare war without authorizing the President to use military force in the conflict. In light of that reality, § 1811 necessarily contemplates a situation in which Congress has both declared war *and* authorized the use of military force—and even that double authorization permits only fifteen days of warrantless electronic surveillance. Where, as here, Congress has seen fit only to authorize the use of military force—and not to declare war—the President cannot assert that he has been granted *more* authority than when Congress declares war as well.

120. 126 S. Ct. 2749 (2006).

Bay Naval Station.[121] The majority opinion concluded that "there is nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth in Article 21 of the UCMJ."[122] In the absence of such "specific, overriding authorization,"[123] the Court found that Congress had not displaced the limits on the President's authority to constitute military commissions that it had previously established with the passage of the UCMJ, a comprehensive scheme subjecting such commissions to the laws of war, including the Geneva Conventions.[124] With respect to the TSP, a similarly comprehensive scheme regulated wiretapping for foreign-intelligence surveillance, and there is similarly "nothing . . . even hinting" at a congressional intent to change that scheme in the text or legislative his-

---

121. *Id.* at 2759

122. *Id.* at 2775.

123. *Id.*

124. The concurring opinions reinforce the notion that such a judicial interpretation best protects the integrity of our political system in times of crisis:

> This is not a case, then, where the Executive can assert some unilateral authority to fill a void left by congressional inaction. It is a case where Congress, in the proper exercise of its powers as an independent branch of government, and as part of a long tradition of legislative involvement in matters of military justice, has considered the subject of military tribunals and set limits on the President's authority. Where a statute provides the conditions for the exercise of governmental power, its requirements are the result of a deliberative and reflective process engaging both of the political branches. Respect for laws derived from the customary operation of the Executive and Legislative Branches gives some assurance of stability in time of crisis. The Constitution is best preserved by reliance on standards tested over time and insulated from the pressures of the moment.
>
> These principles seem vindicated here, for a case that may be of extraordinary importance is resolved by ordinary rules.

Id. at 2799 (Kennedy, J., concurring, joined by Souter, Ginsburg, Breyer, JJ.). Indeed, the same four justices concluded that holding the President accountable to law also strengthens our nation's ability to deal with danger:

> The dissenters say that today's decision would "sorely hamper the President's ability to confront and defeat a new and deadly enemy." They suggest that it undermines our Nation's ability to "preven[t] future attacks" of the grievous sort that we have already suffered. That claim leads me to state briefly what I believe the majority sets forth both explicitly and implicitly at greater length. The Court's conclusion ultimately rests upon a single ground: Congress has not issued the Executive a "blank check." Indeed, Congress has denied the President the legislative authority to create military commissions of the kind at issue here. Nothing prevents the President from returning to Congress to seek the authority he believes necessary.
>
> Where, as here, no emergency prevents consultation with Congress, judicial insistence upon that consultation does not weaken our Nation's ability to deal with danger. To the contrary, that insistence strengthens the Nation's ability to determine—through democratic means —how best to do so. The Constitution places its faith in those democratic means. Our Court today simply does the same.

Id. (Breyer, J., concurring, joined by Souter, Ginsburg, JJ.) (alteration in original) (citations omitted).

tory of the AUMF.[125]

The argument that the AUMF somehow amended FISA belies any reasonable understanding of legislative intent. An amendment to FISA of the sort that would be required to authorize the NSA program would be a significant statutory development, undoubtedly subject to serious legislative debate. It is decidedly *not* the sort of thing that Congress would enact *inadvertently, and without having previously mentioned.* As the Supreme Court recently noted, "Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes."[126]

The government acknowledged that its statutory-authorization argument based on the AUMF would require the conclusion that Congress implicitly repealed several sections of 18 U.S.C. § 2511.[127] Section 2511(2)(f) identifies FISA and specific criminal code provisions as "the *exclusive* means by which electronic surveillance . . . may be conducted." In addition, § 2511 makes it a crime to conduct wiretapping except as "*specifically provided in this chapter*,"[128] or as authorized by FISA.[129] The AUMF is neither in this chapter (i.e. part of Title III, the 1968 Wiretap Act) nor an amendment to FISA, and, therefore, to find that it authorized electronic surveillance would require an implicit repeal of all the above provisions of 18 U.S.C. § 2511.

Repeals by implication are strongly disfavored and can be established only by "overwhelming evidence" that Congress intended the repeal.[130] With respect to the AUMF and FISA there is no such evidence. The Supreme Court has instructed that "the only permissible justification for a repeal by implication is when the earlier and later statutes are irreconcilable."[131] Section 2511 and the AUMF are fully reconcilable. The former makes clear that specified existing laws are the "exclusive means" for conducting electronic surveillance, and that conducting wiretapping outside that specified legal regime is a crime. The AUMF authorizes only such force as is "necessary and *appropriate*."[132] Accordingly, there is no basis whatsoever, let alone the "overwhelming

125. *Id.* at 2775 (Stevens, J.).

126. Gonzales v. Oregon, 546 U.S. 243, 267 (2006) (quoting Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 468 (2001)) (internal quotation marks omitted).

127. *See* DOJ Memo, *supra* note 59, at 36 n.21.

128. 18 U.S.C. § 2511(1) (2000) (emphasis added).

129. *Id.* § 2511(2)(e).

130. J.E.M. Ag Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc., 534 U.S. 124, 137 (2001).

131. *Id.* at 141–42 (quoting Morton v. Mancari, 417 U.S. 535, 550 (1974)) (internal quotation marks omitted).

132. Authorization for the Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified as amended at 50 U.S.C. § 1541).

evidence" required, for overcoming the strong presumption against implied repeals.

The administration's own statements and actions contradicted its claim that the AUMF afforded it authority to conduct warrantless wiretaps. As noted above, Attorney General Gonzales admitted that the administration did not seek to amend FISA to authorize the NSA spying program because some members of Congress advised the administration that it would be "difficult, if not impossible."[133] The administration cannot argue, on the one hand, that Congress authorized the NSA program in the AUMF, and, on the other, that it did not ask Congress for such authorization because it would be "difficult, if not impossible" to get it.

Other actions by the administration also contradicted its subsequent assertion that the AUMF authorized warrantless wiretapping of Americans. Five weeks after the AUMF was signed, Congress explicitly amended FISA in several respects when it passed the USA PATRIOT Act.[134] Congress subsequently amended FISA again two months later, extending from twenty-four to seventy-two hours the emergency-warrant provision of 50 U.S.C. § 1805(f).[135] In doing so Congress specifically found that the seventy-two-hour period was adequate for the preparation of FISA warrant applications in emergency conditions.[136] Yet, there would have been little need for these amendments if the AUMF had already given the President the power to conduct unlimited warrantless electronic surveillance in terrorism cases. Nor was there any discussion in Congress at the time the PATRIOT Act was passed, or when FISA was subsequently amended, acknowledging the administration's view that the AUMF made FISA irrelevant for a whole category of foreign-intelligence electronic surveillance. These amendments of FISA undercut the contention that the President had already been given even broader powers under the AUMF.[137]

---

133. Gonzales/Hayden, *Press Briefing*, *supra* note 1.

134. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of U.S.C.).

135. Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314 (a)(2)(B), 115 Stat. 1394, 1402 (2001).

136. The House and Senate Conference Committee found, "The conferees agreed to a provision to extend the time for judicial ratification of an emergency FISA surveillance or search from 24 to 72 hours. That would give the Government adequate time to assemble an application without requiring extraordinary effort by officials responsible for the preparation of those applications." H.R. REP. No. 107-328, at 23 (2001) (Conf. Rep.), *as reprinted in* 2002 U.S.C.C.A.N. 1217, 1224.

137. In addition, one of the amendments the administration was contemplating seeking in 2002, in a draft bill leaked to the press entitled the "Domestic Security Enhancement Act of 2003," would have amended 50 U.S.C. § 1811 to extend its fifteen-day authorization for warrantless wiretapping to situations where Congress had not declared war but only "authorize[d]

IV. Is It Possible To Have Judicial Review of the Administration's Program of Warrantless Electronic Surveillance in the Face of the Government's Assertion of the State-Secrets Privilege?

In litigation over the TSP, the government responded to the complaints by the various plaintiffs by invoking the state-secrets privilege and moving to dismiss the lawsuits on the ground that the program's secrecy made judicial review of the program impossible.[138] In its crudest formulation, this argument suggests that the President has unilateral power to violate the law and then to block any judicial oversight of his actions by asserting that his violation of law was a secret. The government's specific argument was that:

> adjudication of the merits of their challenge to the TSP would inherently require the disclosure of a range of classified information as to which the Director of National Intelligence has properly asserted the state secrets privilege in this case, including facts that would confirm or deny whether the Plaintiffs were subject to surveillance under the TSP, as well as facts concerning the operation of the TSP and the

---

the use of military force," or where the nation had been attacked. *See* Domestic Security Enhancement Act of 2003 § 103, at 1–2 (Jan. 9, 2003), *available at* http://www.pbs.org/now/politics/patriot2-hi.pdf. If, as the administration later contended, the AUMF gave the President unlimited authority to conduct warrantless wiretapping of the enemy, it would make no sense to seek such an amendment.

138. The government filed a series of affidavits and briefs on the public record and others in camera to justify the assertion of the privilege. In *Center for Constitutional Rights v. Bush*, Civil Action No. 07-1115, this included the public filings of: (1) Memorandum of Points and Authorities in Support of the United States' Assertion of the Military and State Secrets Privilege; Defendants' Motion To Dismiss or, in the Alternative, for Summary Judgment; and Defendants' Motion To Stay Consideration of Plaintiffs' Motion for Summary Judgment, Ctr. for Constitutional Rights v. Bush, No. 06-CV-313 (S.D.N.Y. filed Jan. 17, 2006) [hereinafter Memorandum of Points and Authorities]; (2) Declaration of John D. Negroponte, Director of National Intelligence, *Ctr. for Constitutional Rights*, No. 06-CV-313; (3) Declaration of Major General Richard J. Quirk, Signals Intelligence Director, NSA, *Ctr. for Constitutional Rights*, No. 06-CV-313; (4) Defendants' Reply in Support of Motion To Dismiss or, in the Alternative, for Summary Judgment, *Ctr. for Constitutional Rights*, No. 06-CV-313. The government also made the following classified submissions in support of its motions for the Court's *in camera, ex parte* review: (1) *In Camera, Ex Parte* Classified Memorandum of Points and Authorities in Support of the United States' Assertion of the Military and State Secrets Privilege; Defendants' Motion to Dismiss or, in the Alternative, Motion for Summary Judgment; Defendants' Motion to Stay Consideration of Plaintiffs' Motion for Summary Judgment, *Ctr. for Constitutional Rights*, No. 06-CV-313; (2) *In Camera, Ex Parte,* Classified Declaration of John D. Negroponte, Director of National Intelligence; *Ctr. for Constitutional Rights*, No. 06-CV-313 and (3) *In Camera, Ex Parte* Classified Declaration of Major General Richard J. Quirk, Signals Intelligence Director, National Security Agency, *Ctr. for Constitutional Rights*, No. 06-CV-313. In the MDL proceedings before Judge Vaughn, the government also filed an additional classified declaration by Lieutenant General Keith B. Alexander, who is, the Director of the National Security Agency, for the Court's *in camera, ex parte* review. Defendants' Supplemental Memorandum in Support of Motion To Dismiss or for Summary Judgment, *supra* note 35, at 5 n.6 (citations omitted).

> specific nature of the al Qaeda threat that it sought to address. In particular, if this case proceeded to the merits, state secrets demonstrating precisely what the TSP entailed, and why those activities were reasonable and necessary to meet the al Qaeda theat [sic], would be essential to any determination as to whether the TSP was within the President's statutory and constitutional authority, but could not be disclosed without causing exceptionally grave harm to national security.[139]

The state-secrets privilege may be invoked to shield secret information from discovery and, in rare cases, to dismiss lawsuits if litigation is not possible without disclosing state secrets.[140] Dismissal of claims (or an entire lawsuit) is proper only in two narrow circumstances. First, dismissal may be proper if the "very subject matter" of the lawsuit is itself a state secret.[141]

Second, a case may be dismissed on state-secrets grounds if a court determines, after consideration of non-privileged evidence, that plaintiff cannot present a prima-facie case or that the government cannot present a valid defense without resort to privileged evidence.[142] Even then, dismissal on the basis of the privilege is proper only if the court determines that there is no alternative procedure that would protect secrets but still allow the claims to go forward in some way. Accordingly, courts must use "creativity and care" to devise "procedures which will protect the privilege and yet allow the merits of the controversy to be decided in some form."[143] Suits may be dismissed under the privilege "[o]nly when no amount of effort and care on the part of the court and the parties will safeguard privileged material."[144]

Under a broad view of the state-secrets doctrine, the government

---

139. Defendants' Supplemental Memorandum in Support of Motion To Dismiss or for Summary Judgment, *supra* note 35, at 6 (citations omitted).

140. *See generally* Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931 (2007); William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, POL. SCI. Q., Spring 2005, at 85.

141. *See* Tenet v. Doe, 544 U.S. 1, 9 (2005); United States v. Reynolds, 345 U.S. 1, 11 n.26 (1953); DTM Research, L.L.C. v. AT&T Corp., 245 F.3d 327, 333–34 (4th Cir. 2001) ("[U]nless the very question upon which the case turns is itself a state secret, or the circumstances make clear that sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters, the plaintiff's case should be allowed to proceed . . . ." (quoting Fitzgerald v. Penthouse Int'l, Ltd., 776 F.2d 1236, 1241–42 (4th Cir. 1985)) (citation and internal quotation marks omitted).

142. *See* Molerio v. FBI, 749 F.2d 815, 822, 826 (D.C. Cir. 1984) (terminating suit only after evaluating plaintiffs' nonprivileged evidence and defendant's evidence); Ellsberg v. Mitchell, 709 F.2d 51, 64 n.55 (D.C. Cir. 1983) (remanding where district court had dismissed case on basis of privilege but refusing to consider if plaintiffs could make a *prima facie* case lacking the privileged information).

143. *Fitzgerald*, 776 F.2d at 1238 n.3.

144. *Id.* at 1244.

could immunize executive action from judicial scrutiny. Separation-of-powers principles, however, compel the conclusion that the executive branch cannot disable, by unilateral fiat, the power of Article III courts to be the ultimate arbiters of the law and the Constitution.[145] The Supreme Court has stated that "when the President takes official action, the Court has the authority to determine whether he has acted within the law."[146] To allow the Executive to have the first and final say on the extent of its own power flies in the face of the most basic separation-of-powers principles.[147] In *Hamdi v. Rumsfeld*, the Supreme Court rejected claims of unilateral-executive power with respect to holding enemy combatants in wartime and declared that "[w]hatever power the United States Constitution envisions for the Executive" in wartime, it surely "envisions a role for all three branches when individual liberties are at stake."[148]

As a general matter, courts are plainly competent to review cases implicating even the most sensitive national-security issues, and have done so routinely. In the past five years, in cases related to the same "war on terror" that the government invokes to preclude judicial review of the TSP, courts have decided whether the President can detain enemy combatants captured on the battlefield in Afghanistan and whether those captured are entitled to due process,[149] whether individuals detained at Guantánamo Bay can challenge their detention,[150] and whether these detainees may be subjected to trials not conforming to rules set by Congress.[151] In the past, courts have determined whether the military can try individuals detained inside and outside zones of conflict during times of hostility and peace;[152] whether the government could prevent newspa-

145. *Cf.* United States v. Morrison, 529 U.S. 598, 616 n.7 (2000) ("No doubt the political branches have a role in interpreting and applying the Constitution, but ever since *Marbury* this Court has remained the ultimate expositor of the constitutional text."); Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is.").

146. Clinton v. Jones, 520 U.S. 681, 703 (1997); *see also* Sterling v. Constantin, 287 U.S. 378, 401 (1932) ("What are the allowable limits of military discretion, and whether or not they have been overstepped in a particular case, are judicial questions.").

147. *Jones*, 520 U.S. at 699 ("The Framers 'built into the tripartite Federal Government . . . a self-executing safeguard against the encroachment or aggrandizement of one branch at the expense of the other.'") (quoting Buckley v. Valeo, 424 U.S. 1, 122 (1976) (alteration in original)); Duncan v. Kahanamoku, 327 U.S. 304, 322 (1946) ("[The Framers] were opposed to governments that placed in the hands of one man the power to make, interpret and enforce the laws.").

148. 542 U.S. 507, 536 (2004).

149. *Id.* at 509–10.

150. Rasul v. Bush, 542 U.S. 466, 470 (2004).

151. Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2759 (2006).

152. *E.g.*, United States *ex rel.* Toth v. Quarles, 350 U.S. 11 (1955) (court martial proceedings in Korea); Madsen v. Kinsella, 343 U.S. 341 (1952) (commissions in occupied Germany); *Ex*

pers from publishing the Pentagon Papers because it would allegedly harm national security;[153] whether the executive branch, in the name of national security, could deny passports to members of the Communist Party;[154] whether U.S. civilians outside of the country could be tried by court-martial;[155] whether the President could seize the steel mills during a labor dispute when he believed steel was needed to fight the Korean War;[156] whether the Executive could continue to detain a loyal Japanese American citizen under a war-related executive order;[157] whether the President could block southern ports and seize ships bound for Confederate ports during Civil War;[158] and whether the President could authorize the seizure of ships on the high seas in a manner contrary to an act of Congress during a conflict with France.[159] It would seem that if courts were able to decide these cases, judicial review of the TSP should not be precluded.[160]

Courts have a special duty to review executive action that threatens fundamental liberties. As Judge Cardamone recently warned, "[w]hile everyone recognizes national security concerns are implicated when the government investigates terrorism within our Nation's borders, such concerns should be leavened with common sense so as not forever to trump the rights of the citizenry under the Constitution."[161] As the Fourth Circuit has noted, "[a] blind acceptance by the courts of the government's insistence on the need for secrecy . . . would impermissibly compromise the independence of the judiciary and open the door to pos-

---

parte Quirin, 317 U.S. 1 (1942) (German saboteurs tried by military commission); *Duncan*, 327 U.S. 304 (military trial of civilians in Hawaii); *Ex parte* Milligan, 71 U.S. (4 Wall.) 2 (1866) (civilian in Indiana tried by military commission).

153. N.Y. Times Co. v. United States, 403 U.S. 713 (1971).

154. Kent v. Dulles, 357 U.S. 116 (1958).

155. Reid v. Covert, 354 U.S. 1 (1957).

156. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

157. *Ex parte* Endo, 323 U.S. 283 (1944).

158. The Brig Amy Warwick (The Prize Cases), 67 U.S. (2 Black) 635 (1863).

159. Little v. Barreme, 6 U.S. (2 Cranch) 170 (1804).

160. Courts also routinely handle classified evidence in criminal cases. *See* Classified Information Procedures Act, 18 U.S.C. app. 3 §§ 1–16 (2000 & Supp. IV 2004); United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998) (reviewing classified materials in detail). Courts decide whether to force disclosure of national-security information in FOIA cases. *See, e.g.*, Halpern v. FBI, 181 F.3d 279, 300 (2d Cir. 1999) (rejecting government's Exemption 1 claim). And courts review classification decisions to independently determine whether information is properly classified. *See, e.g.*, McGehee v. Casey, 718 F.2d 1137, 1148 (D.C. Cir. 1983) (requiring de novo judicial review of pre-publication classification determinations to ensure that information is properly classified and agency justified censorship with specificity and agency demonstrated a rational connection between the information and the reasons for the agency's classification"); *see also* Snepp v. United States, 444 U.S. 507, 513 n.8 (1980) (requiring judicial review of pre-publication classification determinations).

161. Doe v. Gonzales, 449 F.3d 415, 423 (2d Cir. 2006) (Cardamone, J., concurring) (emphasis omitted).

sible abuse."[162]

The Supreme Court outlined the proper use of the state-secrets privilege fifty years ago in *United States v. Reynolds*,[163] and has not considered the doctrine in depth since then. In *Reynolds*, the family members of three civilians who died in the crash of a military plane in Georgia sued for damages.[164] In response to a discovery request for the flight-accident report, the government asserted the state-secrets privilege, arguing that the report contained information about secret-military equipment that was being tested aboard the aircraft during the fatal flight.[165] The *Reynolds* Court upheld the claim of privilege over the accident report, but did not dismiss the suit. Rather, it remanded the case for further proceedings, explaining "[t]here is nothing to suggest that the electronic equipment, in this case, had any causal connection with the accident. Therefore, it should be possible for respondents to adduce the essential facts as to causation without resort to material touching upon military secrets."[166] On remand, the case continued with limited discovery (depositions of surviving crew members) and eventually settled.[167]

The privilege is "not to be lightly invoked," nor is it to be "lightly accepted."[168] As one court has cautioned, "the contours of the privilege for state secrets are narrow, and have been so defined in accord with uniquely American concerns for democracy, openness, and separation of powers."[169] Courts have recognized that the privilege is more properly invoked on an item-by-item basis, and not with respect to overbroad categories of information.[170]

In the majority of cases since *Reynolds*, courts have considered the state-secrets privilege in response to particular discovery requests, not as the basis for wholesale dismissal of legal claims concerning the facial legality of a government program. Thus, the typical result of the suc-

---

162. *In re* Wash. Post Co., 807 F.2d 383, 392 (4th Cir. 1986).

163. 345 U.S. 1, 6–8 (1953).

164. *Id.* at 2–3.

165. *Id.* at 3–4.

166. *Id.* at 11.

167. *See* Herring v. United States, No. 03-CV-5500-LDD, 2004 U.S. Dist. LEXIS 18545 at *6, *37 (E.D. Pa. Sept. 10, 2004).

168. *Reynolds*, 345 U.S. at 7, 11; *see also* Jabara v. Kelley, 75 F.R.D. 475, 481 (E.D. Mich. 1977).

169. *In re* Grand Jury Subpoena Dated August 9, 2000, 218 F. Supp. 2d 544, 560 (S.D.N.Y. 2002); *see also In re* United States, 872 F.2d 472, 478–79 (D.C. Cir. 1989) ("Because evidentiary privileges by their very nature hinder the ascertainment of the truth, and may even torpedo it entirely, their exercise 'should in every instance be limited to their narrowest purpose.'" (quoting Barry A. Stulberg, Comment, *State Secrets Privilege: The Executive Caprice Runs Rampant*, 9 LOY. L.A. INT'L & COMP. L. REV. 445, 445 n.5 (1987)); *Jabara*, 75 F.R.D. at 480 ("[C]laims of executive privilege . . . must be narrowly construed . . . .").

170. *See, e.g.*, *In re* United States, 872 F.2d at 478.

cessful invocation of the state-secrets privilege is simply to remove the privileged evidence from the case but to permit the case to proceed.[171]

Outright dismissal of a suit on the basis of the privilege, and the resultant "denial of the forum provided under the Constitution for the resolution of disputes is a drastic remedy."[172] Accordingly, courts have refused to dismiss suits prematurely based on the government's unilateral assertion that state secrets are necessary and relevant to adjudicating all of the claims—particularly without first considering all non-privileged evidence.[173] Similarly, courts have refused to dismiss cases based on the privilege where the purported state secrets are not relevant or necessary to the parties' claims or defenses or where it appears that the parties can proceed with non-privileged evidence.[174] Thus, courts have

171. Many courts have allowed cases to proceed in some form, and often to a merits resolution, despite the invocation of the privilege. *See, e.g.*, *Reynolds*, 345 U.S. at 11 (remanding for further discovery and normal proceedings); DTM Research, L.L.C. v. AT&T Corp. 245 F.3d 327, 334 (4th Cir. 2001) (rejecting a "categorical rule mandating dismissal" whenever the government invokes the state-secrets privilege in a litigation and remanding the case for further proceedings after upholding a claim of privilege to quash a subpoena); Monarch Assurance P.L.C. v. United States, 244 F.3d 1356, 1364 (Fed. Cir. 2001) (upholding CIA's privilege claim in contract action involving alleged financing of clandestine CIA activity, but remanding for further discovery because the lower court prematurely in resolving when national security bars a valid suit); Ellsberg v. Mitchell, 709 F.2d 51, 66–70 (D.C. Cir. 1983) (upholding part of privilege claim but remanding for merits determination); Jabara v. Webster, 691 F.2d 272, 274, 280 (6th Cir. 1982) (deciding case on merits despite prior successful claim of privilege); Attorney Gen. v. The Irish People, Inc., 684 F.2d 928, 955 (D.C. Cir. 1982) (upholding invocation of the privilege but declining to dismiss the case); Heine v. Raus, 399 F.2d 785, 791 (4th Cir. 1968) (upholding claim of privilege in defamation suit, but remanding for further discovery of non-privileged evidence); *Jabara*, 75 F.R.D. at 489, 493 (upholding part of privilege claim but going forward with decision on the merits); *see also* Spock v. United States, 464 F. Supp. 510, 519–20 (S.D.N.Y. 1978) (rejecting as premature pre-discovery motion to dismiss Federal Tort Claims Act suit against the NSA on state secrets grounds); Foster v. United States, 12 Cl. Ct. 492 (1987) (upholding privilege but declining to dismiss). Even in *Halkin v. Helms*, the court allowed the parties to fight "the bulk of their dispute on the battlefield of discovery" and did not dismiss the case out of hand. 690 F.2d 977, 984 (D.C. Cir. 1982).

172. Fitzgerald v. Penthouse Int'l, Ltd., 776 F.2d 1236, 1242 (4th Cir. 1985) (citation omitted); *see also In re United States*, 872 F.2d at 477 ("Dismissal of a suit [on state-secrets grounds at any point of the litigation], and the consequent denial of a forum without giving the plaintiff her day in court . . . is indeed draconian."); *Spock*, 464 F. Supp. at 519 ("An aggrieved party should not lightly be deprived of the constitutional right to petition the courts for relief.").

173. *See, e.g.*, *Monarch Assurance*, 244 F.3d at 1364–65; *In re United States*, 872 F.2d at 477; *Spock*, 464 F. Supp. at 519–20.

174. *See, e.g.*, Crater Corp. v. Lucent Techs., Inc., 423 F.3d 1260, 1269 (Fed. Cir. 2005) (reversing dismissal on the basis of the privilege where the nonprivileged record was not sufficiently developed and the relevancy of any privileged evidence was unclear); *Monarch Assurance*, 244 F.3d at 1364 (reversing dismissal on state-secrets grounds so that plaintiff could engage in further discovery to support claim with nonprivileged evidence); Clift v. United States, 597 F.2d 826, 830 (2d Cir. 1979) (remanding for further proceedings where plaintiff has "not conceded that without the requested documents he would be unable to proceed, however difficult it might be to do so"); *Heine*, 399 F.2d at 791 (upholding claim of privilege in defamation suit, but remanding for further discovery of non-privileged evidence).

routinely rejected a "categorical rule mandating dismissal whenever the state secrets privilege is validly invoked."[175]

In only two cases has the Supreme Court dismissed a matter on the pleadings. Both involved claims under alleged contracts to carry out espionage; in both, the Court held that the very nature of such contracts implied secrecy terms that "preclude[ ] any action for their enforcement."[176] The Supreme Court's decisions in *Reynolds* and *Totten* thus spawned two separate doctrines: first, "the state secrets privilege, which is an evidentiary and discovery rule that . . . is not applicable at the pleading stage[,]" and that, when validly claimed, results only in nondisclosure of the particular evidence sought.[177] Second, a public-policy doctrine based on *Totten* that calls for dismissal of those very few cases in which sensitive military secrets will be so central to the subject matter of the case that any effort to proceed with the litigation will threaten disclosure of privileged matters.[178]

The Ninth Circuit held that the very subject matter of the actions filed to enjoin the TSP should not be considered a state secret because the government has publicly acknowledged, described, and defended the challenged surveillance program.[179] The government not only acknowledged the existence and scope of the TSP but engaged in an aggressive

175. *DTM Research*, 245 F.3d at 334.

176. Totten v. United States, 92 U.S. 105, 107 (1875); *see also* Tenet v. Doe, 544 U.S. 1, 9 (2005) ("[L]awsuits premised on alleged espionage agreements are altogether forbidden.").

177. Hudson River Sloop Clearwater, Inc. v. Dep't of the Navy, No. CV-86-3292, 1989 U.S. Dist. LEXIS 19034, at *4 (E.D.N.Y. May 1, 1989).

178. *See* Fitzgerald v. Penthouse Int'l, Ltd., 776 F.2d 1236, 1241–44 (4th Cir. 1985) (characterizing the power to dismiss cases when "very subject matter" is a state secret as "narrow"). An example is *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991). That case arose out of an attack on a U.S. vessel in an area of conflict (the 1987 U.S.S. Stark disaster in the Persian Gulf), and the plaintiffs' claims were directed at "design, manufacture, performance, [and] functional characteristics" of state-of-the-art military equipment, and military "rules of engagement." *Id.* at 547. Courts are traditionally hesitant to entertain claims questioning tactical practices of the armed forces on the battlefield, and a number of immunities might well have shielded defendants had the case not been dismissed on the pleadings. For example, the private defendants argued that "courts should not entertain tort actions arising out of the engagement of United States armed forces in areas of hostility" and also that dismissal was warranted because the claims were being pursued against Iraq by the United States. *See* Zuckerbraun v. Gen. Dynamics Corp., 755 F. Supp 1134, 1136 & n.2 (D. Conn. 1990), *aff'd*, 935 F.2d 544 (2d Cir. 1991).

179. Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1198 (9th Cir. 2007); *see also* Doe v. Gonzales, 449 F.3d 415, 423 (2d Cir. 2006) ("[T]he [Plaintiffs'] identities . . . were published, yet the government continued to insist that . . . [they] may not identify themselves and that their identities must still be kept secret. This is like closing the barn door after the horse has already bolted.") (Cardamone, J., concurring); Capital Cities Media, Inc. v. Toole, 463 U.S. 1303, 1306 (1983) ("[The Court] ha[s] not permitted restrictions on the publication of information that would have been available to any member of the public . . . ."); Snepp v. United States, 444 U.S. 507, 513 n.8 (1980) (suggesting that government would have no interest in censoring information already "in the public domain"); Virginia Dep't of State Police v. Wash. Post, 386 F.3d 567, 579

public-relations campaign to convince the American public that the program was both lawful and necessary to protect national security. On January 19, 2006, the Department of Justice issued a forty-two page White Paper discussing in detail its legal defenses and justifications for the TSP.[180] Government officials publicly testified before Congress about the legality, scope, and basis for the NSA surveillance several times.[181] President Bush discussed and promoted the TSP at least eight times through radio addresses, at news conferences, and at public events.[182] Vice President Cheney promoted the TSP during a commencement address at the U.S. Naval Academy[183] and at four separate rallies for servicemen and servicewomen.[184] Administration officials have even participated in public-web discussions in defense of the TSP.[185] The administration ensured that its defense of the program received the broadest possible public exposure. Having done those things, it should not be allowed to insulate its actions from judicial oversight by arguing that the very subject matter of the cases challenging the TSP is a state secret.

In similar contexts, courts have properly rejected privilege claims

(4th Cir. 2004) (holding that government had no compelling interest in keeping information sealed where the "information ha[d] already become a matter of public knowledge").

180. *See* DOJ Memo, *supra* note 59.

181. *See Operations of the Department of Justice: Hearing Before the H. Comm. on the Judiciary*, 109th Cong. 37–40, 42–44 (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States); *Nomination of General Michael V. Hayden, USAF, To Be the Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. (2006); *Hearings*, *supra* note 18 (statement of Alberto Gonzales, Att'y Gen. of the United States); *Worldwide Terror Threat: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. (2006) (statement of John Negroponte, Director of National Intelligence and Gen. Michael Hayden, then Principal Deputy Director of National Intelligence).

182. *See* President's Radio Address, 42 WEEKLY COMP. PRES. DOC. 926 (May 13, 2006); Remarks on the Terrorist Surveillance Program, 42 WEEKLY COMP. PRES. DOC. 911 (May 11, 2006); President's News Conference, 42 WEEKLY COMP. PRES. DOC. 125, 128–29 (Jan. 26, 2006); Remarks Following a Visit to the National Security Agency at Fort Meade, Maryland, 42 WEEKLY COMP. PRES. DOC. 121, 122–23 (Jan. 25, 2006); Remarks on the War on Terror and a Question-and-Answer Session in Manhattan, Kansas, 42 WEEKLY COMP. PRES. DOC. 101, 109 (Jan. 23, 2006); Remarks on the War on Terror and a Question-and-Answer Session in Louisville, Kentucky, 42 WEEKLY COMP. PRES. DOC. 40, 46–47 (Jan. 11, 2006); President's News Conference, *supra* note 1; President's Radio Address, *supra* note 1.

183. Vice President Richard Cheney, Commencement Address at the United States Naval Academy (May 26, 2006).

184. Vice President Richard Cheney, Rally for the Troops at Fairchild Air Force Base (Apr. 17, 2006); Vice President Richard Cheney, Remarks at a Rally for the Troops at Scott Air Force Base (Mar. 21, 2006); Vice President Richard Cheney, Remarks at a Rally for the Troops at Charleston Air Force Base (Mar. 17, 2006); Vice President Richard Cheney, Remarks at a Rally for the Troops at Fort Leavenworth (Jan. 6, 2006).

185. In January 2006, for example, Attorney General Gonzales conducted a web discussion—part of the White House's online interactive forum called "Ask the White House"—where he answered questions from members of the public regarding the NSA program. Attorney General Alberto Gonzales, *supra* note 15.

over information that has already been widely publicized. In *Spock*, for example, the court rejected the claim that the NSA could not admit or deny that plaintiffs' communications had been intercepted without harm to national security, finding that this would "reveal[ ] no important state secret" particularly because it had already been disclosed in the *Washington Post*.[186] The court went on to hold that dismissal of plaintiffs' action was wholly inappropriate "where the only disclosure in issue [was] the admission or denial of the allegation that interception of communications occurred[,] an allegation which ha[d] already received widespread publicity the abrogation of the plaintiff's right of access to the courts could undermine our country's historic commitment to the rule of law."[187] Similarly, in *Jabara v. Kelley*, the district court observed that where information over which the government asserted the privilege had been revealed in a report to Congress—specifically that it was the NSA that had intercepted plaintiffs' communications—"it would be a farce to conclude" that information "remain[ed] a military or state secret."[188]

The focus of the challenge to the TSP is not a secret at all—the question presented is a basic constitutional-law question that should be decided on the basis of first principles. The two Supreme Court decisions of greatest relevance to the constitutionality of the TSP, *Youngstown* and *Keith*, resolved similar issues of presidential power without recourse to state secrets. In *Youngstown* the constitutionality of the President's action in seizing the steel mills was considered at a fundamental and principled level—whether the "Commander in Chief of the Armed Forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production."[189] There was no reference in the constitutional analysis to precisely what products were produced in the factories seized, what their importance was to national defense, what weapons and ammunition the military in Korea had on hand, what battlefield information (secret or otherwise) relevant to the need to produce additional munitions, how the factories seized were operated by the government, or any other factual details.

In *Keith*, the Court was able to resolve the question whether the

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

187. *Id.* at 520.

188. 75 F.R.D. 475, 493 (E.D. Mich. 1977); *see also In re* United States, 872 F.2d 472, 478 (D.C. Cir. 1989) (rejecting privilege claim, relying in part on prior release under the Freedom of Information Act of information relevant to litigation); Ellsberg v. Mitchell, 709 F.2d 51, 61 (D.C. Cir. 1983) (rejecting portion of privilege claim on ground that so much relevant information was already public).

189. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587 (1952).

President had constitutional authority to conduct electronic surveillance of domestic threats to national security without recourse to state secrets.[190] The constitutional analysis was not perceived to depend on the nature and extent of domestic threats to national security, the methods of operation available to the government short of warrantless electronic surveillance, the kind of electronic-surveillance methods available to the government and the deployment tactics, or any similar presumably secret matters. The Court noted the government's assertion that there had been 1562 bombing incidents in the United States in the first half of 1971, most at government institutions, and concluded, "[t]he precise level of this activity, however, is not relevant to the disposition of this case."[191] The records of the Supreme Court and the lower courts in *Youngstown* and *Keith* are devoid of any suggestion that state secrets were essential to the important constitutional questions decided in those cases.[192]

The Circuit Courts of Appeals in *United States v. Clay*,[193] *United States v. Brown*,[194] *United States v. Butenko*,[195] and *United States v. Truong Dinh Hung*[196] ruled on the President's implied power to conduct warrantless electronic surveillance in national-security cases without access to state secrets. The government did not argue, even in the most recent of those cases, that the question of the President's constitutional authority could not be resolved without state-secrets information.[197] The court perhaps most likely to recognize the state-secrets argument—the FISA Court—made no reference to it, and instead simply took for granted that the power existed.[198] The government relied on these cases for its claim that the TSP was constitutional. The government's argument, however, both that there is persuasive precedent that such surveillance was constitutional and that courts cannot decide the question without access to state secrets that were not available in the previous cases, is fatally inconsistent.

---

190. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 324 (1972).

191. *Id.* at 311 n.12.

192. Similarly, in *Little v. Barreme*, the Supreme Court required no secret information about the particular conflict between the United States and France, or about the specific danger posed by ships coming from France, to hold that Congress had "prescribed . . . the manner in which th[e] law shall be carried into execution." 6 U.S. (2 Cranch) 170, 177–78 (1804). As a result of its analysis of the text of the statute, the Court concluded that the President had no authority to seize ships bound from France, as opposed to bound to France. *Id.* at 178.

193. 430 F.2d 165 (5th Cir. 1970), *rev'd*, 403 U.S. 698 (1971).

194. 484 F.2d 418 (5th Cir. 1973).

195. 494 F.2d 593 (3d Cir. 1974).

196. 667 F.2d 1105 (4th Cir. 1981).

197. *See* Brief for the United States, United States v. Humphrey, 667 F.2d 1105 (4th Cir. 1981) (No. 76-5176), 1979 WL 212414.

198. *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (per curiam).

The mere fact that a suit concerns a classified-intelligence program does not transform the very subject matter of the suit into a state secret. No court has ever relied on the state-secrets privilege to dismiss purely legal claims concerning the facial validity of a government-surveillance program.[199] Numerous cases that involve harms flowing from covert or clandestine programs or activity have been the subject of litigation, and often, even where the privilege is validly invoked over some evidence, the case has been allowed to proceed in some form.[200] Indeed, courts that have considered challenges to warrantless surveillance have not considered the very subject matter a state secret, even where the plaintiffs were challenging NSA surveillance.[201]

Further, numerous courts have adjudicated legal questions regarding foreign-intelligence surveillance without confronting any state-secrets problem. For example, courts have faced no evidentiary or state-secrets obstacle in evaluating the constitutionality of FISA.[202] Indeed, since September 11 courts have evaluated the facial legality of government-surveillance tools without any state-secrets issues arising and without any question regarding their authority to do so.[203] To dismiss the

199. *But cf.* El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007) (affirming dismissal of damages claim by alleged victim of extraordinary-rendition program).

200. *See, e.g.*, Monarch Assurance P.L.C v. United States, 244 F.3d 1356 (Fed. Cir. 2001) (claims involving covert CIA financing); Kronisch v. Gottlieb, No. 99-6152, 2000 WL 534301 (2d Cir. May 2, 2000) (case involving CIA clandestine LSD program); Kronisch v. United States, 150 F.3d 112 (2d Cir. 1998); Air-Sea Forwarders, Inc. v. Air Asia Co., 880 F.2d 176 (9th Cir. 1989) (claims regarding CIA cover company); Birnbaum v. United States, 588 F.2d 319 (2d Cir. 1978) (covert CIA mail-opening program); Heine v. Raus, 399 F.2d 785 (4th Cir. 1968) (defamation case involving covert CIA spies); Linder v. Calero-Portocarrero, 180 F.R.D. 168 (D.D.C. 1998) (wrongful-death action against leaders of Nicaraguan Contra organizations); Orlikow v. United States, 682 F. Supp. 77 (D.D.C. 1988) (claims involving CIA's covert MKULTRA program); Avery v. United States, 434 F. Supp. 937 (D. Conn. 1977) (CIA covert mail-opening program); Cruikshank v. United States, 431 F. Supp. 1355 (D. Haw. 1977); Barlow v. United States, 53 Fed. Cl. 667 (2002) (whistleblower claims involving facts about CIA and nuclear-weapons proliferation).

201. *See, e.g.*, Jabara v. Webster, 691 F.2d 272 (6th Cir. 2982) (deciding claims on the merits even where some aspects of case were state secrets); Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983) (remanding some claims for consideration on the merits, despite upholding privilege claims over particular evidence); Halkin v. Helms (*Halkin I*), 598 F.2d 1 (D.C. Cir. 1978) (dismissing claims against the NSA only after discovery and not because the very subject matter was a state secret); Spock v. United States, 464 F. Supp. 510 (S.D.N.Y. 1978) (refusing to prematurely dismiss claims against the NSA on the basis of the privilege); Jabara v. Kelley, 75 F.R.D. 475 (E.D. Mich. 1977) (ruling on the privilege claims but no suggestion that the very subject matter was a state secret).

202. *See, e.g.*, United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

203. *See, e.g.*, Doe v. Gonzales, 386 F. Supp. 2d 66 (D. Conn. 2006) (evaluating constitutionality of the national-security-letter power in counter-terrorism and counter-intelligence investigations); Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated*, 449 F.3d 415 (2d Cir. 2006) (same).

cases challenging the TSP on the ground that the very subject matter is an alleged state secret would produce a perverse result: Where Congress, by statute, authorizes the Executive to engage in foreign-intelligence gathering, courts may review its legality and constitutionality; but where the Executive secretly violates limits placed by Congress on eavesdropping, a court would be powerless to opine on its legality.[204]

---

204. It is also possible to argue that in enacting FISA, Congress abrogated the state-secrets privilege as a bar to the litigation of claims respecting illegal electronic surveillance. This argument was made by both the Al-Haramain plaintiffs, Al-Haramain Islamic Found., Inc., 507 F.3d 1190, 1205 (9th Cir. 2007), and in *Center for Constitutional Rights v. Bush*, Memorandum in Opposition to Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 28, Ctr. for Constitutional Rights v. Bush, No. 06-cv-313 (S.D.N.Y. filed Jan. 17, 2006.) In *Al-Haramain*, the Ninth Circuit remanded the question to the District Court, which had not reached this issue in its original opinion. 507 F.3d at 1205–06. The argument is based on the fact that Congress created a civil cause of action for violations of FISA, 50 U.S.C. § 1810, and a procedure governing review of the propriety of the process by which a FISA order was sought, 50 U.S.C. § 1806(f). The latter section makes clear that a judge may look past executive affidavits and scrutinize the underlying evidence "relating to the surveillance" in determining whether a disclosure of such information would harm the national security:

> [The court] shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. § 1806(f) (2000); *see also* H.R. Rep. No. 95-1720 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048; S. Rep. No. 95-701, at 64 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 4033 ("The committee views the procedures set forth in [§ 1806(f)] as striking a reasonable balance between an entirely in camera proceeding . . . and mandatory disclosure . . . ."). The D.C. Circuit has suggested that this procedure under § 1806(f) may also be used in suits under FISA's civil-damages-action provision, 50 U.S.C. § 1810. *See* ACLU Found. of So. Cal. v. Barr, 952 F.2d 457, 470 (1991) ("Congress also anticipated that issues regarding the legality of FISA-authorized surveillance would arise in civil proceedings and . . . it empowered federal district courts to resolve those issues . . . .").

Congress's creation of a specific cause of action for a FISA violation necessarily contemplates judicial review of actions taken by the government in violation of FISA. The Second Circuit recognized as much in an opinion holding that the state-secrets privilege was waived with relation to litigation brought under an act allowing an inventor to seek compensation for patents kept secret owing to military necessity:

> The assertion by the United States of its privilege with respect to state secrets is, we think, governed by similar considerations. Congress has created rights which it has authorized federal district courts to try. Inevitably, by their very nature, the trial of cases involving patent applications placed under a secrecy order will always involve matters within the scope of this privilege. Unless Congress has created rights which are completely illusory, existing only at the mercy of government officials, the act [authorizing such claims] must be viewed as waiving the privilege.

Halpern v. United States, 258 F.2d 36, 43 (2d Cir. 1958). By creating causes of action against the government—even going so far as to allow civil-damages claims—in circumstances that would "by their very nature . . . always involve matters within the scope of this privilege" as the government might colorably assert it, Congress acknowledged that the federal courts may entertain actions under FISA, waiving or abrogating the common-law state-secrets privilege with respect to such claims. *Id.*; *see also* Kasza v. Browner, 133 F.3d 1159, 1167 (9th Cir. 1998).

In the litigation over the TSP, the disclosure of state secrets is not necessary to resolve any of the significant issues on the merits. The government admitted that it was engaging in warrantless surveillance covered by FISA and therefore was not following the requirements of the statute. The government offered only one defense to plaintiffs' statutory claim—namely that Congress, through the AUMF, authorized the President to engage in warrantless wiretapping of Americans on American soil. That defense posed a purely legal question: Does one statute, the AUMF, trump two other statutes, FISA and 18 U.S.C. § 2511 (2)(f), which provide that FISA and Title III are the exclusive means for wiretapping Americans?

The government's AUMF defense of its actions turns on statutory construction, not facts—privileged or otherwise. The government devoted the bulk of its forty-two-page memorandum to Congress to arguing this precise point—presumably without disclosing any state secrets. Whether Congress intended the general AUMF to repeal the very specific FISA requirements is a purely legal question. That legal question is controlled by the decision in *Hamdan v. Rumsfeld*.[205]

State secrets are also unnecessary to judicial review of the claim that the President exceeded his authority and violated the separation of powers by intruding on Congress's prerogatives. The government contended that the courts cannot resolve the legal and constitutional questions concerning the TSP without a plethora of facts about the specific nature of the al Qaeda threat, the scope of the program, and the operational details of the surveillance—all of which, it argued, are subject to the state-secrets privilege.

The government suggested that state secrets about "the specific threat facing the Nation and the particular actions taken by the President to meet that threat" would support its claim of inherent authority and provide a valid defense to plaintiffs' claims.[206] But the President has no authority to violate the law, no matter what his motivations may be, and no matter what kind of threat or emergency is posed. The Constitution does not grant the President any emergency powers to ignore the law. In *Youngstown*, Justice Jackson wisely recognized that the Framers were not unaware of emergencies, and yet provided no general relief from constitutional constraints when they occur:

> The appeal, however, that we declare the existence of inherent powers *ex necessitate* to meet an emergency asks us to do what many think would be wise, although it is something the forefathers omitted. They knew what emergencies were, knew the pressures they engen-

205. See *supra*, Part II, for the discussion of *Hamdan*.

206. Memorandum of Points and Authorities, *supra* note 138, at 3.

> der for authoritative action, knew, too, how they afford a ready pretext for usurpation. We may also suspect that they suspected that emergency powers would tend to kindle emergencies. Aside from suspension of the privilege of the writ of habeas corpus in time of rebellion or invasion, when the public safety may require it, they made no express provision for exercise of extraordinary authority because of a crisis. I do not think we rightfully may so amend their work . . . .[207]

The question of the President's constitutional authority must first be resolved by resort to principles, not by analysis of the facts of a specific threat at a specific point in time. As Justice Jackson noted in *Youngstown*, "[t]he opinions of judges, no less than executives and publicists, often suffer the infirmity of confusing the issue of a power's validity with the cause it is invoked to promote . . . . The tendency is strong to emphasize transient results upon policies . . . and lose sight of enduring consequences upon the balanced power structure of our Republic."[208]

V. THE IMPACT OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDERS IN JANUARY 2007

Shortly before the oral argument before the Sixth Circuit Court of Appeals in *ACLU v. NSA*,[209] the government announced that President Bush would not reauthorize the TSP because the government had succeeded in obtaining an order under FISA allowing similar surveillance to be conducted under the Act.[210] Attorney General Gonzales advised the Senate Judiciary Committee:

> [O]n January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.[211]

The Attorney General claimed that the government had been exploring the possibility of conducting the surveillance through the FISA Court

---

207. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 649–50 (1952) (footnotes omitted).

208. *Id.* at 634

209. 493 F.3d 644 (6th Cir. 2007).

210. Gonzales Letter, *supra* note 34.

211. *Id.* para. 1.

even before the existence of the program had been made public. He stated, "[t]hese orders are innovative, they are complex, and it took considerable time and work for the Government to develop the approach that was proposed to the Court and for the Judge on the FISC to consider and approve these orders."[212] He concluded by stating that "the President has determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires."[213]

The orders signed by the FISA Court were not made public. Nor was there ever any public explanation of what was "innovative" or "complex" about the orders, nor why the government could not have taken that approach from the beginning.[214] The government did not explain whether the "innovative" approach deviated in any way from the requirements of the FISA statute.

The government subsequently contended that as a result of the FISA Court orders, the various legal challenges seeking an injunction against the TSP were moot. But the plaintiffs in those actions claimed that their cases were not moot because of the doctrine that a party may not evade judicial review of questionable conduct by voluntarily ceasing such conduct during review.[215] To guard against intentional avoidance of judicial review, the cases hold that the party asserting mootness bears the heavy burden of persuading the court that the challenged conduct cannot reasonably be expected to start up again.[216] The "stringent" burden on a party asserting mootness is to show that "subsequent events ma[k]e it absolutely clear that the alleged wrongful behavior [can] not reasonably be expected to recur."[217]

The government must have recognized that it could not possibly meet this heavy burden, given that it continued to insist that the TSP had been (and continued to be) entirely legal, that the President might reauthorize it in the event that the FISA Court orders were not renewed,[218] and that he might indeed opt out of the regime created by

212. *Id.* para. 2.

213. *Id.* para. 3.

214. In January 2006 the President claimed that it was not possible to conduct this program under the old law (referring to FISA). President's News Conference, *supra* note 182, at 133.

215. *See, e.g.*, Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 174 (2000) ("A defendant's voluntary cessation of allegedly unlawful conduct ordinarily does not suffice to moot a case."); City of Mesquite v. Aladdin's Castle, Inc., 455 U.S. 283, 289 (1982) (same). Otherwise, a party would be free to resume the conduct after a challenge was dismissed as moot, as courts would be compelled to leave the defendant "free to return to his old ways." United States v. Concentrated Phosphate Exp. Ass'n, 393 U.S. 199, 203 (1968) (quoting United States v. W.T. Grant Co., 345 U.S. 629, 632 (1953)).

216. *See Concentrated Phosphate*, 393 U.S. at 203.

217. *Id.*; *see also* Parents Involved in Cmty. Sch. v. Seattle Sch. Dist. No. 1, 127 S. Ct. 2738, 2751 (2007) ("heavy burden"); *Friends of the Earth*, 528 U.S. at 190 ("formidable burden").

218. In *Parents Involved*, the Supreme Court relied on the facts that the Seattle School District,

the new FISA orders at any time he pleases.

Attorney General Gonzales testified before Congress that his "belief is that the actions taken by the administration, by this president, were lawful, in the past."[219] Indeed, notwithstanding the government's implication that the program is no longer in effect because it was allowed to lapse without being reauthorized, the government asserts the right to carry out surveillance under the terms of the program challenged in this lawsuit *at any time*.[220] In fact, the government has claimed that the President not only has the right to carry out such surveillance outside of FISA under the proper circumstances, but that he has the *duty* to do so.[221] In several colloquies at oral argument before the Sixth Circuit, the government agreed with questions suggesting that it could in fact opt out of the FISA Court orders at any time, or indeed conduct surveillance outside of FISA even while the FISA Court orders were in effect.[222] In every respect, then, it appears that the decision to let the NSA Program's

---

a governmental body, "vigorously defends the constitutionality" of the school-assignment program it had ceased using, "and nowhere suggests that if this litigation is resolved in its favor it will not resume" the challenged practice. 127 S. Ct. at 2751. Both factors were present with respect to the TSP.

219. *Oversight of the U.S. Department of Justice: S. Comm. on the Judiciary*, 110th Cong. 38 (2007); *see also* Gonzales Letter, *supra* note 34, para. 3 ("[A]s we have previously explained, the Terrorist Surveillance Program fully complies with the law . . . .").

220. *See* Tony Snow, Press Sec'y, White House, Press Briefing (Jan. 17, 2007) (Q: ". . . the President has always argued that—I mean, he has the ability, he has the authority not to use FISA to get authority" . . . White House Spokesman Snow: "Yes, and he still believes that."), *available at* http://www.whitehouse.gov/news/releases/2007/01/20070117-5.html; Government's Reply in Support of Its Supplemental Submission Discussing the Implications of the Intervening FISA Court Orders of January 10, 2007 at 5, ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, No. 07-468, 2008 WL 423556, at *1 (U.S. Feb. 19, 2008) (No. 06-2095) ("[T]he President has not disavowed his authority to reauthorize the TSP in the event that the FISA court orders are not renewed . . . ."); *Proposed FISA Modernization Legislation: Hearing of the S. Select Comm. on Intelligence* (May 1, 2007) (Sen. Feingold: "Can each of you assure the American people that there is not . . . and will not be any more surveillance in which the FISA process is side-stepped based on arguments that the president has independent authority under Article II or the authorization of the use of military force? / Director of National Intelligence Michael McConnell: "Sir, the president's authority under Article II is—are in the Constitution. So if the president chose to exercise Article II authority, that would be the president's call.").

221. *See, e.g.*, Memorandum of Points and Authorities, *supra* note 138, at 30, 38 (noting that the President's most important power is the obligation to protect the U.S., that the President determined that the FISA process did failed under the current threat, and that this judgment fell within the President's powers).

222. ACLU v. NSA, 493 F.3d 644, 693–720 (6th Cir. 2007) (Gilman, J., dissenting), *cert. denied*, No. 07-468, 2008 WL 423556, at *1 (U.S. Feb. 19, 2008); *see also* Audio File: Oral Argument of ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007) (Jan. 31, 2007), *available at* http://www.ca6.uscourts.gov/internet/06_2095/06_2095.mp3 at 18'45" (Judge Gillman: "But [you can] opt out of the FISA regime whenever you decide to, couldn't you? The FISA court hasn't restrained you from doing that." The Government attorney Coppolino: "That's absolutely true, Your Honor . . . ."); *id.* at 19'53" (Judge Batchelder: "Those aren't the only possibilities. I mean, the possibility also exists, theoretically, at least, that the FISA court would be perfectly willing to reauthorize but that the Executive would nevertheless decide to conduct some surveillance outside

authorization lapse was a matter of executive grace, and that a decision to revive it might have been taken at any time as a matter of executive discretion.

Given that both the TSP and FISA orders are secret, the plaintiffs in the various lawsuits, those who communicate with them, and the public would have no way of knowing whether and when FISA orders expire or if the President reauthorizes non-FISA surveillance.

The government argued that the mootness issue should not be analyzed under the voluntary-cessation argument, but rather under the "capable of repetition, yet evading review" exception to mootness.[223] In that event, the government's "formidable burden" of showing that it is "absolutely clear that the allegedly wrongful behavior could not reasonably be expected to recur,"[224] would disappear, and instead there would be a burden on the plaintiffs in the cases to demonstrate a probability that the same controversy would recur involving the same party. Given the parallels between this case and the voluntary-cessation cases, it was the plaintiffs who had the better of this argument.

VI. WARRANTLESS ELECTRONIC SURVEILLANCE UNDER THE FOURTH AMENDMENT

A. *The 2007 Amendments to FISA*

In August 2007 FISA was amended to give congressional approval to warrantless electronic surveillance for foreign threats to national security. The new legislation dramatically changed the previous statute and departs from the ordinary requirements imposed by the Fourth Amendment. First, the scope of FISA was limited in a new section 105A by excluding from the definition of "electronic surveillance" governed by the statute, "surveillance directed at a person reasonably believed to be located outside of the United States."[225] Second, a new procedure for conducting surveillance and acquiring information "concerning" persons reasonably believed to be outside the United States was created in a new section 105B.[226]

Under § 1805b(a), the Director of National Intelligence (the

---

the FISA court jurisdiction and parameters." Coppolino: "That is true, Your Honor. That is a hypothetical possibility . . . .").

223. *See* Ctr. for Biological Diversity v. Lohn, 483 F.3d 984, 989 (9th Cir. 2007); Native Vill. of Noatak v. Blatchford, 38 F.3d 1505, 1509 (9th Cir. 1994).

224. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 189 (2000) (quoting United States v. Concentrated Phosphate Exp. Ass'n, 393 U.S. 199, 203 (1968)) (internal quotation marks omitted).

225. Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552 (2007) (to be codified at 50 U.S.C. § 1805a).

226. *Id.* § 2, 121 Stat. at 552 (to be codified at 50 U.S.C. § 1805b).

"Director") and the Attorney General are authorized to gather "foreign intelligence information" concerning persons reasonably believed to be outside the United States for a period of up to one year if certain conditions are met.[227] The law requires the Director and the Attorney General to find that there are reasonable procedures in place for determining that the subjects of the surveillance are reasonably believed to be outside the United States and provides that the procedures are subject to review by the FISC.[228] The acquisition may not constitute "electronic surveillance."[229] The acquisition must involve obtaining foreign-intelligence information from or with the assistance of a communications-service provider or other person who has access to communications (either while they are transmitted or stored), or to equipment that may be used to transmit or store communications. A "significant purpose" of the acquisition must be to obtain foreign-intelligence information.[230] Finally, minimization procedures that meet the definition of § 1801(h) of FISA must be used.[231] The Director and the Attorney General must make a written certification under oath that these conditions are met before taking action, unless immediate action is required and time does not permit preparation of the certification. In that event, the certification must be prepared within seventy-two hours.[232]

Unlike the particularity requirement imposed by the Fourth Amendment,[233] the certification "is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed."[234] The certification must be filed "as soon as practicable" with the FISC.[235]

The Director and the Attorney General may direct private-communications personnel to cooperate with them in acquiring information and maintaining the secrecy of the acquisition.[236] In the event that private parties refuse to cooperate with the government, the Director and the Attorney General may seek a court order requiring cooperation, which

227. *Id.*

228. *Id.* As explained *infra*, this review was not likely to occur unless the act is renewed beyond its original 180-day sunset.

229. *Id.* This provision seems tautological, inasmuch as the statute defines persons reasonably believed to be outside the United States as beyond the reach of electronic surveillance.

230. *Id.* § 2, 121 Stat. at 553 (to be codified at 50 U.S.C. § 1805b).

231. *Id.*

232. *Id.*

233. U.S. CONST. amend. IV. ("[A]nd no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

234. Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 553 (to be codified at 50 U.S.C. § 1805b).

235. *Id.*

236. *Id.*

the court must issue if the directive was issued pursuant to the statute and is otherwise lawful.[237] Failure to comply with such an order is punishable as a contempt of court.[238] The recipient of such an order may challenge it by filing a petition with the FISA Court, but the order will not be set aside if it meets the requirements of the statute and is not "otherwise unlawful."[239]

The submission by the Director and the Attorney General to the FISA Court of the procedures for determining that subjects of surveillance are outside the United States is not due for 120 days after the effective date of the Act.[240] The FISA Court is granted 180 days from the effective date of the Act to complete its review of the procedures.[241] The Director and the Attorney General determine whether the procedures are reasonably designed to ensure that the subject of surveillance is reasonably believed to be outside the United States.[242] The FISA Court's review is limited to determining whether the judgment of the Director and the Attorney General is clearly erroneous.[243] If the Court finds that the determination was clearly erroneous, the government has an additional thirty days to amend the procedures.[244] In addition, the government could appeal an adverse decision of the FISA Court to the Court of Review and petition for certiorari to the Supreme Court. Acquisitions of information may continue while appeals are pending.[245]

The August 2007 version of the Act provides that the amendments made by the Act will cease to have effect 180 days after the effective date of the Act, provided that any authorizations made under the Act may continue until their termination.[246] The latter provision would

237. *Id.* § 2, 121 Stat. at 554 (to be codified at 50 U.S.C. § 1805b).

238. *Id.*

239. *Id.* The recipient of the order may further appeal to the Court of Review and petition for a writ of certiorari to the Supreme Court. *Id.*

240. *Id.* § 3, 121 Stat. at 555 (to be codified at 50 U.S.C. § 1805c).

241. *Id.*

242. *Id.*

243. *Id.*

244. *Id.*

245. *Id.*

246. *Id.* § 6, 121 Stat. at 557 (to be codified at 50 U.S.C. § 1803 note). At the time of this writing the August 2007 amendments have been temporarily extended while Congress debates the terms of a new bill to authorize the continuation of this surveillance. It is not possible at this time to determine to what extent the criticisms made here of the 2007 amendments will be relevant to the new legislation. It appears, however, that the version of the pending bill adopted by the House of Representatives has corrected several of the most egregious problems in the 2007 amendments. *See* H.R. 3773, 110th Cong. (as passed by House, Mar. 14, 2008). One significant issue under debate at the time of this writing is whether telecommunications companies will receive retroactive immunity for their participation in the TSP. The ongoing developments with respect to this legislation are closely monitored on the ACLU's website: http://www.aclu.org/safefree/general/17321res20030408.html.

extend the effective sunset of the Act for an additional year. Given the 180-day sunset provision, it seems that the amendment for review by the FISA Court of the procedures established by the Director and the Attorney General is not likely to have any meaning unless the Act is extended.

The new procedures thus permit the acquisition of "foreign intelligence information" of persons reasonably believed to be outside the United States without any court order. "Foreign intelligence information" is defined by the original FISA enactment.[247] The definition is extremely broad. Despite particular references to violent attacks against the United States, the statute is drafted in the disjunctive to include "information with respect to a foreign power or foreign territory that relates to . . . (b) the conduct of the foreign affairs of the United States."[248] Given that definition, there would seem to be no limitation on warrantless surveillance aimed at gathering commercial, financial, or even sports and entertainment information if it would affect the conduct of the foreign affairs of the United States.

B. *The Original Terrorist Surveillance Program Under the Fourth Amendment*

The Fourth Amendment imposes an independent limit on the power of the government to engage in electronic surveillance without a judicial warrant. No theory of implied-executive power asserts that the President can take actions that are proscribed by explicit provisions of the constitution.

As the Supreme Court recognized in *United States v. United States District Court* (*Keith*), private, confidential communications are protected by the Fourth Amendment, and are essential to the exercise of First Amendment freedoms of speech, association, and petition.[249] The warrant and probable-cause requirements serve to protect both privacy

247. 50 U.S.C. § 1801(e) (2000) defines "foreign intelligence information" as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

248. 50 U.S.C. § 1801(e)(2).

249. 407 U.S. 297, 313–14 (1972).

and speech interests. The Court recognized that First and Fourth Amendment rights are the most likely to be imperiled in national security cases:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. . . . History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.[250]

Keith held that probable cause and a warrant were required for electronic surveillance authorized by the Attorney General, on behalf of the President, of domestic persons who allegedly constituted a threat to the national security. The *Keith* Court recognized that exceptions to the warrant requirement are "few in number and carefully delineated,"[251] and it refused to accept the government's argument that the circumstances of domestic-security surveillances constituted grounds to establish a new exception for such cases. The Court specifically rejected the government's arguments that requiring prior judicial review would obstruct the President in the exercise of his duty to protect national security; that such surveillance was exempt from the Fourth Amendment because it was directed primarily to collecting and maintaining intelligence with respect to subversive forces and not for criminal prosecutions; that the warrant requirement was not intended to restrain ongoing intelligence gathering as compared to criminal investigations; that courts would not have sufficiently sophisticated knowledge or techniques to assess whether such surveillance was necessary to protect national security; and that disclosures to judicial officers would compromise the security of informants and agents and the secrecy necessary for intelligence gathering.[252]

The *Keith* Court explicitly did not decide whether the Constitution forbids warrantless electronic surveillance of foreign powers or their agents in national-security cases. But its reasoning nonetheless strongly

250. *Id.* (citation omitted).
251. *Id.* at 318 (citing Katz v. United States, 389 U.S. 347, 357 (1967)).
252. *Id.* at 318–20.

supports the conclusion that a warrant is required for electronic surveillance of foreign agents as well.

The requirement that a neutral, disinterested magistrate be involved in the process of instituting surveillance reflects the basic constitutional premise that executive officers cannot be trusted to police themselves where the privacy rights of individuals are concerned.[253] The "indiscriminate wiretapping and bugging of law-abiding citizens" that the *Keith* Court rightly feared are no less likely simply because the targets of such surveillance are suspected of being affiliated with a foreign power.[254] There is no reason that the executive's institutional tendency to undervalue privacy and err on the side of intrusions should be diminished where the targets of the investigation are suspected of being foreign agents; if anything, executive officers can be expected to err in favor of surveillance even more markedly when investigating threats they believe to be foreign, because the officers may not believe Americans' rights are at stake. Relying on NSA-shift supervisors to safeguard the privacy rights of Americans resurrects the precise evil against which the Fourth Amendment was directed by "plac[ing] the liberty of every man in the hands of every petty officer."[255]

The principal rationale advanced by the administration for squaring the TSP with the Fourth Amendment is unpersuasive. The Justice Department contended that the TSP can be justified under a line of Fourth Amendment cases permitting searches without warrants and probable cause in order to further "special needs" above and beyond ordinary law enforcement.[256] The Supreme Court has recognized, however, that "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers."[257]

The Court has used the special-needs doctrine to uphold highway drunk-driving checkpoints, finding them reasonable because they are standardized, the stops are very brief and only minimally intrusive, and a warrant and probable-cause requirement would defeat the purpose of

253. *Katz*, 389 U.S. at 358–59 ("[B]ypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations 'only in the discretion of the police.'" (citation omitted)); *Keith*, 497 U.S. at 317 ("The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised." (footnote omitted)).

254. *Keith*, 497 U.S. at 321.

255. Stanford v. Texas, 379 U.S. 476, 481 (1965) (quoting James Otis's description of the British writs of assistance in *Boyd v. United States*, 116 U.S. 616, 625 (1886)) (internal quotation marks omitted).

256. DOJ Memo, *supra* note 59, at 37–41.

257. New Jersey v. T.L.O., 469 U.S. 325, 351 (1985).

keeping drunk drivers off the road.[258] Similarly, the Court has upheld school drug-testing programs under the special-needs doctrine, finding them reasonable because students have diminished expectations of privacy in school, the programs are limited to students engaging in extracurricular programs (so students have advance notice and the choice to opt out), and the drug testing is standardized and tests only for the presence of drugs.[259]

The TSP had *none* of the safeguards found critical to upholding special-needs searches in these contexts. All the special-needs cases contain certain elements: impracticability of the warrant or probable-cause requirement; standardized testing or notice or an opportunity not to participate in the test-invoking activity or both; and most significantly, a minimal intrusion on privacy because the search takes place in a setting where expectations of privacy are reduced (because it involves either students in a secondary school, voluntary participation in certain activities, probation, a high security and highly regulated job).[260] Unlike a minimally intrusive brief stop on a highway or a urine test, the TSP consisted of wiretapping telephone and e-mail communications—searches of a sort the Supreme Court has found to be among the most intrusive available to the government.[261] The TSP was not standardized,

258. Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

259. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995).

260. *See T.L.O.*, 469 U.S. at 327 (students in secondary school); *Acton*, 515 U.S. at 648 (voluntary participation in certain activities); Bd. of Educ. v. Earls, 536 U.S. 822, 831 (2002) (same); Griffin v. Wisconsin, 483 U.S 868 (1987) (probation); United States v. Knights, 534 U.S. 112 (2001) (same); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989) (high security and highly regulated job); Skinner v. Ry. Labor Executives' Ass'n., 489 U.S. 602 (1989) (same).

261. Electronic eavesdropping "[b]y its very nature . . . involves an intrusion on privacy that is broad in scope." Berger v. New York, 388 U.S. 41, 56 (1967). It therefore bears a dangerous "similarity to the general warrants out of which our Revolution sprang." *Id.* at 64 (Douglas, J., concurring). Indeed, "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." *Id.* at 63 (majority opinion). Unlike physical search warrants allowing for one limited intrusion, the *Berger* court found that the New York wiretapping statute at issue allowed "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause." *Id.* at 59. Any number of conversations might be seized, "over a prolonged and extended period[,]" with any number of parties eavesdropped upon even if only one is the target of the surveillance. *Id.* at 57. The statute allowed "no termination date on the eavesdrop once the conversation sought is seized." *Id.* at 59–60. And "because [wiretapping's] success depends on secrecy, [the statute had] no requirement for notice" of a wiretap order. *Id.* at 60.

For all these reasons the *Berger* Court implied that lawful electronic-surveillance orders would have to adhere to judicially supervised safeguards to minimize the impact of the surveillance on privacy—including limits on duration of the surveillance, and some form of showing that no other, less-intrusive means were available that might allow law enforcement to acquire the same information. *Id.* ("Such a showing of exigency, in order to avoid notice would appear more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized."). Congress recognized the

but subject to discretionary targeting under a standard and process that remain secret. Those whose privacy is intruded on had no notice or choice to opt out of the surveillance. And it was neither limited to the environment of a school nor analogous to a brief stop for a few seconds at a highway checkpoint.

Unless the Supreme Court was prepared to expand the scope of the special-needs exception beyond the sorts of cases to which it was previously applied, the TSP should be considered as unconstitutional under the warrant requirement of the Fourth Amendment.

There is no greater need for state secrets to resolve the constitutional question under the Fourth Amendment with respect to the TSP than there was in *Keith*, where the Court held warrantless electronic surveillance of domestic threats to national security unconstitutional without regard to state secrets.[262] In *Ellsberg v. Mitchell*, the D.C. Circuit rejected the government's argument that state secrets necessarily prevented the government from arguing that there was a foreign-intelligence exception to the warrant requirement. The court stated that there was "no reason to relieve those who authorize and conduct [warrantless foreign-intelligence taps] of the burden of showing that they come within the exemption."[263] As the court explained,

> In many such situations, the government would be able (as it has been here) to refuse to disclose any details of the circumstances surrounding the surveillance by invoking its state secrets privilege. The result would be to deny the plaintiffs access to all of the information they need to dispute the government's characterization of the nature and purpose of the surveillance. And the net effect would be to immunize, not only all wiretaps legitimately falling within the hypothesized "foreign agent" exemption, but all other surveillance conducted with equipment or under circumstances sufficiently sensitive to permit assertion of the state secrets privilege. We find such consequences unacceptable.[264]

In fact, the court went on to note that such a consequence "might call into question the very existence of the foreign agent exception."[265]

---

constitutional dimension of these minimization requirements in both Title III and FISA. *See* 50 U.S.C. § 1804(a)(5) (2000) (mandating that applications and orders under FISA include a statement of proposed minimization procedures).

262. The Court in *Keith* did note the government's assertion, apparently based on non-secret information, that there had been 1562 bombing incidents in the United States in the first six months of 1971, most at government facilities, but concluded that the precise level of that activity was "not relevant to the disposition of this case." United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 311 n.12 (1972).

263. 709 F.2d 51, 68 (D.C. Cir. 1983).

264. *Id.* (footnote omitted).

265. *Id.*

Accordingly, because the defendants had not yet made any showing regarding the existence and application of any foreign-intelligence exception to the warrant requirement, the court refused to dismiss those claims and remanded to the district court. The court noted that the remaining questions were primarily "questions of law" that could be resolved in camera if necessary.[266]

C. *The 2007 Amendments to FISA Under the Fourth Amendment*

The 2007 amendments to FISA eliminated any argument that Congress has not authorized the President to conduct the surveillance of communications contemplated by the statute without a warrant. The President is now acting in Justice Jackson's first category in his *Youngstown* concurrence, under an express authorization by Congress, where presidential authority is at its maximum.[267] As a practical matter, the only serious remaining question about the legality of the program is whether it complies with the requirements of the Fourth Amendment.

The question whether FISA is constitutional under the Fourth Amendment brings the inquiry back to primacy of the warrant requirement discussed at length in *Keith*. Throughout the controversy over the NSA warrantless electronic surveillance, the government argued that the essential Fourth Amendment requirement is that a search be "reasonable," not whether it is conducted pursuant to a warrant.[268] But this argument ignores the teaching of *Keith*, that "'reasonableness' derives content and meaning through reference to the warrant clause."[269] *Keith* explicitly rejected the argument that reasonableness was a substitute for a judicial warrant:

> Some have argued that "[t]he relevant test is not whether it is reasonable to procure a search warrant, but whether the search was reasonable[.]" This view, however, overlooks the second clause of the Amendment. The warrant clause of the Fourth Amendment is not dead language. Rather, it has been
>
> > "a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be

266. *Id.* at 69–70; *see also* Jabara v. Webster, 691 F.2d 272, 276 (6th Cir. 1982) ("[D]efendants had divulged the interception and later transmittal to the FBI . . . . Thus . . . the state secret privilege was no impediment to the adjudication of [plaintiff's] fourth amendment claim."); Jabara v. Kelley, 75 F.R.D. 475, 489 (E.D. Mich. 1977) (upholding Attorney General's claim of privilege, and pointing out afterward that the "matter ha[d] not ended" because the court still had to determine "whether the warrantless electronic surveillances . . . compl[ied] with the commands of the Fourth Amendment").

267. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 634–38 (1952).

268. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 300 (1972).

269. *Id.* at 309–10 (citing Coolidge v. New Hampshire, 403 U.S. 443, 473–84 (1971)).

> somehow 'weighed' against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' who are a part of any system of law enforcement."[270]

The Court noted that the argument that reasonableness was the test "has not been accepted."[271] The Court quoted *Chimel v. California*, where the Court had concluded that the argument was "founded on little more than a subjective view regarding the acceptability of certain sorts of police conduct, and not on considerations relevant to Fourth Amendment interests" and, that "[u]nder such an unconfined analysis, Fourth Amendment protection in this area would approach the evaporation point."[272]

Notwithstanding the government's arguments in the NSA-surveillance cases and elsewhere, *Keith*'s insistence on the primacy of the warrant requirement is still the law.[273] Although there are exceptions to the warrant requirement, they continue to be "few in number and carefully delineated."[274]

The argument that an inquiry into reasonableness has supplanted the warrant requirement is based on isolated references to reasonableness in cases dealing with exceptions to the warrant requirement.[275] In *Illinois v. McArthur*, for example, the Court stated that the "central requirement" of the Fourth Amendment is "one of reasonableness."[276] It further stated that the rules and regulations established to enforce that requirement "[s]ometimes . . . require warrants."[277] In the same case, however, the Court made it clear that in "the ordinary case" seizures are "unreasonable within the meaning of the Fourth Amendment, without more, unless . . . accomplished pursuant to a judicial warrant, issued by a

---

270. *Id.* at 315–16 (quoting *Coolidge*, 403 U.S. at 481).

271. *Id.* at 315 n.16 (citing Chimel v. California, 395 U.S. 752, 764–65 (1969)).

272. 395 U.S. at 764–65.

273. *See* Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 785 (2004) ("In a long series of cases, however, the Supreme Court has made it clear that almost all searches and seizures require a prior warrant issued with probable cause, and that law enforcement may act without a warrant only in certain circumstances that have been defined categorically and narrowly.").

274. 407 U.S. at 318 (citing Katz v. United States, 389 U.S. 347, 357 (1967)).

275. The government made such arguments in *Center for Constitutional Rights v. Bush* in their initial brief in support of its motion to dismiss or for summary judgment. Memorandum of Points and Authorities, *supra* note 138.

276. 531 U.S. 326, 330 (citing Texas v. Brown, 460 U.S. 730 (1983)).

277. *Id.*

neutral magistrate after finding probable cause."[278] The Court then described searches and seizures conducted without warrants in the face of "special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like" as "exceptions to the warrant requirement."[279] The Court ultimately held that no warrant was necessary to detain McArthur and prevent him from entering his home while they sought a warrant to search it for drugs, because of the exigent circumstances presented by the risk that he would destroy the evidence if he entered the home alone. In the face of the exigent-circumstances argument, the Court declined to find the seizure per se unreasonable, and proceeded to balance the privacy-related and law-enforcement-related competing concerns to determine whether the officers' actions were reasonable.[280] The Court did not, however, abandon the warrant requirement as the threshold inquiry.

That the "central requirement" of the Fourth Amendment is reasonableness comes from Chief Justice Rehnquist's plurality opinion in *Texas v. Brown*.[281] A majority of the Justices wrote concurring opinions criticizing the understated role afforded the warrant requirement in the Rehnquist opinion.[282]

As recently as last term, in an opinion by Chief Justice Roberts, the Court continued to analyze a search under the "warrant requirement," noting that it is a "basic principle of Fourth Amendment law that

278. *Id.* (quoting United States v. Place, 462 U.S. 696, 701 (1983)) (internal quotation marks omitted).

279. *Id.*

280. *Id.* at 331. The cases relied on for this balancing approach in *McArthur* involved vehicle stops. *See* Delaware v. Prouse, 440 U.S. 648, 654 (1979) (random spot checks of vehicles on road are not constitutional); United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975) (roving border patrol stops not constitutional in absence of reasonable suspicion). In *Prouse*, the Court noted that "the Warrant Clause of the Fourth Amendment generally requires that prior to a search a neutral and detached magistrate ascertain that the requisite standard is met." 440 U.S. at 654 n.11.

281. 460 U.S. at 739.

282. Justices Powell and Blackmun did not join the plurality opinion because it "appear[ed] to accord less significance to the Warrant Clause of the Fourth Amendment than is justified by the language and purpose of that Amendment." *Id.* at 744 (Powell, J., concurring). Their opinion cites the numerous Supreme Court opinions emphasizing that exceptions to the warrant requirement are "few in number and carefully delineated." *Id.* at 745 (quoting *Keith*, 407 at 318) (internal quotation marks omitted). But they also note that "the opinions of this Court in Warrant Clause cases have not always been consistent. They have reflected disagreement among Justices as to the extent to which the Clause defines the reasonableness standard of the Amendment." *Id.* at 745.

Justices Stevens, Brennan, and Marshall also concurred, for the reason that the plurality opinion had given "inadequate consideration" to the warrant requirement. *Id.* at 747 (Stevens, J., concurring). Justice Stevens concluded that "the Warrant Clause embodies our government's historical commitment to bear the burden of inconvenience. Exigent circumstances must be shown before the Constitution will entrust an individual's privacy to the judgment of a single police officer." *Id.* at 750.

searches and seizures inside a home without a warrant are presumptively unreasonable."[283] The Court did not supplant the warrant requirement with a general balancing test for reasonableness.

In *Keith*, Justice Powell emphasized the historical provenance of the warrant requirement, referencing Lord Mansfield's decision in 1765 that warrants for seditious libel must name the person to be arrested, and not leave the decision of who should be arrested to the judgment of the arresting officer.[284] He concluded that:

> Lord Mansfield's formulation touches the very heart of the Fourth Amendment directive: that, where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation. Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate."[285]

The Court in *Keith* rejected the argument that the president could unilaterally authorize surveillance in domestic national-security cases, concluding, "[T]he Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates."[286] This is based on the "historical judgment, which the Fourth Amendment accepts . . . that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[287]

The Framers drafted the Fourth Amendment to protect privacy for the benefits that ensuring a realm of private life brings. The development of personality that is possible when one is able to live unobserved by government watchers and the exchange of ideas and emotions that is possible when one can communicate with others without observation by government agents are examples of these benefits. The benefits of protecting privileged communications are familiar to all lawyers. The benefits accrue only where there is confidence that one's privacy is as protected as possible, as inviolate as the Constitution and laws permit.

---

283. Brigham City, Utah v. Stuart, 126 S. Ct. 1943, 1947 (2006) (citation and internal quotation marks omitted). The Court noted that the "ultimate touchstone" of the Fourth Amendment was reasonableness and hence there are exceptions to the warrant requirement. *Id.*

284. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 316 (1972) (citing Leach v. Three of the King's Messengers, 19 How. St. Tr. 1001, 1027 (K.B. 1765)).

285. *Id.* (citing Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971) and Katz v. United States, 389 U.S. 347, 356 (1967)).

286. *Id.* at 317.

287. *Id.*; *see also* McDonald v. United States, 335 U.S. 451, 455–56 (1948) ("The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of individuals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.").

The particularity requirement, for example, is designed to limit government intrusions into private spaces (now understood to include conversations) and to permit searching or surveillance of conversations only where evidence or fruits of crime or unprivileged conversations with foreign agents will be discovered. Cognizant of these limitations, a free person is entitled to confidence that private spaces and communications that fall outside the government's permitted zone of search and observation will remain private.

This is why the scope of Fourth Amendment protections is based on "reasonable expectation of privacy."[288] It is noteworthy that this concept was first articulated in *Katz*, an electronic-surveillance case. As the Court concluded, "a person in a telephone booth may *rely upon* the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely *entitled to assume* that the words he utters into the mouthpiece will not be broadcast to the world."[289] It is the ability to rely on the protection of the Fourth Amendment, to assume that one is not being overheard, that is significant, because in the absence of that reliance one cannot feel free to express private thoughts.

The 2007 amendments to FISA pose an even weaker argument for application of the special-needs exception to the warrant requirement than did the TSP. To justify an exception to the warrant requirement for special needs, the solution must be a "reasonably effective" means for addressing the problem that justifies recourse to the exception.[290] The courts have not required that the means chosen are the least-restrictive alternative to solving the problem and have afforded some measure of discretion to the judgment of law-enforcement officials.[291] Nonetheless, there is, as Justice Ginsburg put it, "a difference between imperfect tailoring and no tailoring at all."[292]

The 2007 FISA amendments permit the warrantless electronic surveillance of any person reasonably believed to be outside the United States for the purpose of gathering foreign-intelligence information. As described above, this includes any "information with respect to a foreign power that relates to . . . the conduct of the foreign affairs of the United

288. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

289. *Id.* at 352 (majority opinion) (emphasis added).

290. *See, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 837 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 660 (1995) (analyzing the "efficacy of th[e] means" for meeting the problem); Gould & Stern, *supra* note 273, at 826–28.

291. *See, e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 453–54 (1990) ("[F]or purposes of Fourth Amendment analysis, the choice among such reasonable alternatives remains with the governmental offices who have a unique understanding of, and a responsibility for, limited public resources, including a finite number of police officers.").

292. *Earls*, 536 U.S. at 852 (Ginsburg, J., dissenting).

States."[293] The purported justification for warrantless surveillance under the FISA amendments is the protection of the United States from terrorists, principally al Qaeda and its supporters. A statute that permits conversations between any person abroad with information that relates to the conduct of U.S. foreign affairs and a citizen of the United States within this country to be overheard without a judicial warrant is simply not a "reasonably effective" means of addressing the terrorism problem. The breadth of the 2007 FISA amendments disqualifies them from coming within the special-needs exception to the warrant requirement.

The 2007 FISA amendments also fail to comply with Fourth Amendment requirements because they invest standardless and unrestrained discretion in the hands of the government agents who make decisions about who to target for surveillance.[294] The Court carefully reviewed inspection protocols in *Skinner v. Railway Executives Ass'n*,[295] and *National Treasury Employees Union v. Von Raab*[296] to ensure that inspections were done randomly, or that all persons were tested, and that officials had no discretion about how to administer the tests.[297] In *Delaware v. Prouse*, the Court invalidated automobile stops where the officers had "standardless and unconstrained discretion."[298]

The searches contemplated by the 2007 FISA amendments are subject to no guidelines or standards other than that the subject of surveillance is reasonably believed to be outside the United States and in possession of foreign-intelligence information. Unlike the original FISA provisions, the 2007 amendments do not limit surveillance to those who are an "agent of a foreign power."[299] That provision in the original version of FISA had limited the subjects of surveillance, as noted by the Foreign Intelligence Court of Review:

> Under the definition of "agent of a foreign power" FISA surveillance could not be authorized against an American reporter merely because he gathers information for publication in a newspaper, even if the information was classified by the Government. Nor would it be authorized against a Government employee or former employee who reveals secrets to a reporter or in a book for the purpose of informing

293. 50 U.S.C.S. § 1801(e)(2) (Lexis 2007).

294. *See* New York v. Burger, 482 U.S. 691, 711–12 (1987) (upholding warrantless searches in automobile junkyard because administrative-inspection program limited discretion of officers).

295. 489 U.S. 602, 621–22 (1989).

296. 489 U.S. 656, 6687, 672 n.2 (1989).

297. *See* Gould & Stern, *supra* note 273, at 818–19.

298. *Id.* 440 U.S. 648, 661 (1979); *see also* City of Indianapolis v. Edmond, 531 U.S. 32, 49 (2000) (Rehnquist, C.J., dissenting) ("Roadblock seizures are consistent with the Fourth Amendment if they are 'carried out pursuant to a plan embodying explicit, neutral limitations on the conduct of individual officers.'" (quoting Brown v. Texas, 443 U.S. 47, 51 (1979)).

299. 50 U.S.C. § 1801(b) (2000).

> the American people. This definition would not authorize surveillance of ethnic Americans who lawfully gather political information and perhaps even lawfully share it with the foreign government of their national origin. It obviously would not apply to lawful activities to lobby, influence, or inform Members of Congress or the administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information preparatory to such lawful activities.
>
> . . . As should be clear from the foregoing, FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security.[300]

Under the amendments, the persons described in the previous paragraph could become the subject of surveillance. The amendments do not limit warrantless surveillance to "carefully delineated, and particularly serious, foreign threats to national security."[301]

In the absence of review of proposed searches by an impartial judicial officer, limitations on the discretion of the authorizing law-enforcement agents are crucial. The failure to include any meaningful limitations in the 2007 FISA amendments is fatal to any argument that warrantless searches under the amendments can be justified under the special-needs exception.

VII. CONCLUSION

Over the course of American history, Presidents have periodically asserted the right to take unilateral action based on claims that national security demanded it, and have overreached in doing so, violating basic constitutional rights. History has always rendered a judgment that a terrible mistake was made. We have learned that executive overreaching often has posed a risk as great or greater to our democratic way of life than the dangers such officials warned against.

The TSP and the 2007 amendments to FISA raise fundamental questions about the implied powers of the President and the powers of the government in general to conduct warrantless electronic surveillance. This article has made the argument that the President's actions with respect to warrantless electronic surveillance are illegal and unconstitutional. The government has argued that the judicial branch is precluded from entertaining those questions because of the state-secrets privilege. The government's argument would render even blatant constitutional violations immune from judicial inquiry once an executive

300. *In re* Sealed Case, 310 F.3d 717, 739 (FISA Ct. Rev. 2002).
301. *Id.*

official announces that, in his opinion, disclosures necessary to the litigation of a case would somehow harm national security.

That argument is fundamentally incompatible with the structure of American democracy. Our divided system of government can only function when the courts are willing to hold the Executive to account for breaking the law. The permanent damage that would be caused by the abject abandonment of our constitutional system of checks and balances and separation of powers is incalculably greater than any temporal danger that might be presumed to exist to our national security from external enemies.

Two extraordinary cases demonstrate the need for judicial scrutiny of executive overreaching despite asserted national-security concerns. In *Korematsu v. United States*, the Supreme Court upheld the wholesale transportation and internment in camps of the Japanese American population on the West Coast because it concluded it could not "reject as unfounded" the conclusion of the military authorities that there was the "gravest imminent danger to the public safety."[302] Forty years later, both congressional and judicial authorities documented that the Department of Justice had been in possession of information contradicting General DeWitt's report, on which the Supreme Court relied, and that the government's brief in the Supreme Court had been redrafted twice to keep that fact from the Court.[303] The commission established by Congress to study the matter concluded that the detention of the Japanese Americans was caused not by military necessity, but by "race prejudice, war hysteria and a failure of political leadership."[304] *Korematsu* occupies some of the most shameful pages in the United States Reports.

At the other end of the spectrum of judicial review lies the Pentagon Papers case, *New York Times Co. v. United States*.[305] The government claimed that national security required an order forbidding the *New York Times* and the *Washington Post* from publishing a classified study concerning the Vietnam War already in their possession. The Supreme Court rejected the argument and the papers were published, with no adverse consequences to national security.[306] Cases such as these should leave us all skeptical of the broad claims of secrecy the Executive makes under the banner of national security in the shadow of September 11.

---

302. 323 U.S. 214, 218 (1944).

303. Korematsu v. United States, 584 F. Supp. 1406, 1416–17 (N.D. Cal. 1984).

304. *Id.* at 1417.

305. 403 U.S. 713 (1971).

306. The Solicitor General Erwin Griswold, who argued for secrecy, later admitted that he had opposed publication although he had perceived no threat to national security. Erwin N. Griswold, *Secrets Not Worth Keeping*, WASH. POST, Feb. 15, 1989, at A25.