Warrantless Wiretapping: The Bush Administration's Failure to Jam an Elephant into a Mousehole

by ADRIENNE RATNER*

> [T]his concept of "national defense" cannot be deemed an end in itself, justifying any exercise of legislative power designed to promote such a goal. Implicit in the term "national defense" is the notion of defending those values and ideals which set this Nation apart. For almost two centuries, our country has taken singular pride in the democratic ideals enshrined in its Constitution.... It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties... which make the defense of the Nation worthwhile.
>
> *Chief Justice Earl Warren (1967)*[1]

Introduction

In 2005, *The New York Times* revealed that the National Security Agency ("NSA") had been illegally targeting hundreds of thousands of domestic telephone and e-mail communications for surveillance since 2002.[2] Allegedly necessary in order to gather intelligence on al

---

* J.D. Candidate 2010, University of California, Hastings College of the Law. Special thanks to Professor Elizabeth Hillman, Matt Chayt, and Sarah Crespi for their comments and inspiring discussions.

1. United States v. Robel, 389 U.S. 258, 264 (1967).

2. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* www.nytimes.com/2005/12/16/politics/16program/html?_r=1&pagewanted=all.

The day following the *New York Times* story, President George W. Bush confirmed the existence of a "'terrorist surveillance program" in his weekly radio address: "In the weeks following the [September 11, 2001] 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 Qaeda and related

Qaeda, this program of dragnet surveillance, authorized by President George W. Bush without the consent of Congress and referred to as the "terrorist surveillance program" ("TSP"),[3] circumvented the Foreign Information Surveillance Act ("FISA"), which requires the executive branch to obtain a judicial order prior to or within fifteen days of initiating a wiretap.[4] For four years, until *The New York Times* revealed the warrantless wiretapping, President Bush reauthorized the TSP every forty-five days at the recommendation of the intelligence community and Department of Justice memoranda.[5]

On July 10, 2009, exactly one year after Congress authorized FISA Amendments in 2008, the Inspectors General of five federal security and intelligence agencies and the Department of Justice released an unclassified report concluding that FISA's requirements had not hindered intelligence gathering efforts.[6] Nonetheless—in fact, now with even more vigor—the Obama Administration continues to support the Bush Administration's illegal, pointless wiretapping program,[7] which, though codified into law in 2008,[8]

---

terrorist organizations. Before we intercept these communications, the Government must have information that establishes a clear link to these terrorist networks." ACLU v. NSA, 493 F.3d 644, 648 n.1 (6th Cir. 2007).

3. The Inspectors General of the Justice Department, the Defense Department, the Central Intelligence Agency, the National Security Agency and the Office of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program*, July 10, 2009, *available at* http://documents.nytimes.com/federal-report-on-the-president-s-surveillance-program#p=1 [hereinafter *Surveillance Program Report*].

4. 50 U.S.C. § 1811. "The President's authorization of the NSA program appeared to contravene both FISA's criminal prohibition on statutorily unauthorized electronic surveillance, and another statutory provision specifying that FISA's procedures are to be the 'exclusive means' by which such surveillance can be lawfully performed for foreign intelligence purposes. Senator Arlen Specter, chair of the Senate Committee on the Judiciary, immediately questioned the legality of the program, and announced that his committee would hold hearings on the issue early in the new year. The Bush Administration responded with an aggressive public relations campaign . . . ." David Cole & Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Framing the Debate*, 81 IND. L.J. 1355, 1355 (2006).

5. Editorial, *Illegal, and Pointless*, N.Y. TIMES, July 17, 2009, at A22, *available at* http://www.nytimes.com/2009/07/17/opinion/17fri1.html?_r=3.

6. "Most [intelligence community] officials interviewed . . . had difficulty citing specific instances where PSP reporting had directly contributed to counterterrorism successes." *Surveillance Program Report*, *supra* note 3, at 40.

7. Brief for the United States as Amicus Curiae Supporting Respondent, Mohawk Industries, Inc. v. Norman Carpenter, No. 08-678, pp. 28-32, *available at* http://www.abanet.org/publiced/preview/briefs/pdfs/07-08/08678_RespondentAmCuUSA. pdf. On August 2, 2009, in a case largely about attorney client privilege, the Obama Administration filed an amicus brief asserting the broad power of the state secrets power to shut down lawsuits and arguing that the state secrets privilege was rooted in the

remains unconstitutional. In the only federal lawsuit challenging the legality of the TSP, the Obama Administration has argued that the court should not review previously released documents that prove illegal domestic surveillance.[9] Furthermore, the Obama

---

Constitution. *See also* Editorial, *Still Wrong on Wiretapping*, S.F. CHRON., July 20, 2009, at A10 Bob Egelko, *Obama Goes to Bat for Bush Wiretap Program,* S.F. CHRON., July 16, 2009, at A6 Adam Liptak, *Obama Administration Weighs in on State Secrets, Raising Concern on the Left,* N.Y. TIMES, Aug. 3, 2009, at A11

As a senator and presidential candidate, Barack Obama voted for FISA 2008. At the time, Senator Obama expressed that he was unsatisfied with the immunity provision and pledged he would "work to remove this provision so that we can seek full accountability for past offenses."

Contrary to Presidential Candidate Obama's campaign statements, the Obama Administration has tenaciously and rigorously defended the TSP and tried to prevent any judicial ruling that the Bush Administration TSP was illegal: "President Obama has refused to open a full investigation of the many laws that were evaded, twisted or broken —pointlessly and destructively—under Mr. Bush. Mr. Obama should change his mind. A full accounting is the only way to ensure these abuses never happen again." Editorial, *supra* note 5.

8. *See* 50 U.S.C. § 1801 (2008). On July 10, 2008, the United States Senate approved by a landslide (69 to 28), and President Bush promptly signed into law, a bill amending the Foreign Intelligence Surveillance Act to permit the government to conduct mass, untargeted surveillance of all communications coming into and out of the United States without any individualized review and without any finding of wrongdoing. Eric Lichtblau, *Senate Approves Bill to Broaden Wiretap Powers*, N.Y. TIMES, July 10, 2008, at A1, *available at* http://www.nytimes.com/2008/07/10/washington/10fisa.html?partner=permalink&exprod=permalink. In addition to permitting warrantless domestic wiretapping to be conducted legally, the FISA 2008 Amendments grant immunity to telecommunications companies and unspecified individuals who may have shared surveillance records with the government at any point in the last seven years. The FISA Amendments of 2008 drastically alter the degree of scrutiny required for domestic electronic surveillance and provide immunity to telecommunications companies that aid the government in conducting electronic surveillance. For Fourth Amendment conflicts, see Legal History and Review of the Foreign Intelligence Surveillance Act, http://www.cnss.org/fisa.htm (last visited Oct. 2, 2009),

9. Glenn Greenwald, *Obama's Efforts To Block a Judicial Ruling on Bush's Illegal Eavesdropping,* SALON, ,Feb. 28 2009, http://www.salon.com/opinion/greenwald/2009/02/28/ al_haramain/index.html ("As part of a criminal investigation against the Al-Haramain Islamic Foundation, an Oregon-based charity, the Bush DOJ accidentally turned over to the charity's lawyers a document showing that the Bush NSA eavesdropped without warrants on conversations between the charity and its two lawyers, both U.S. citizens. The charity and its lawyers then sued the Bush administration for illegally eavesdropping on their communications. That document is what distinguished this case from all other NSA cases, because it enables the plaintiffs (the charity and its lawyers) to prove that they were subjected to Bush's illegal spying program and they therefore have standing to sue. . . ." The Obama Administration seeks to block the court from considering that document.) *See also* David Kravets, *Appeals Court Allows Classified Evidence in Spy Case*, WIRED BLOG NETWORK, Feb. 27, 2009, http://blog.wired.com/27bstroke6/2009/02/appeals-court-a.html; *see also* David Kravets, *Obama Administration: Constitution Does Not Protect Cell-Site Records*, WIRED BLOG NETWORK, Mar. 17, 2009,

Administration has gone even further than the Bush Administration in its assertion of the state secret doctrine, suggesting that it might use the power of state secrets to shut down lawsuits regarding the constitutionality of warrantless wiretapping.[10]

Prior to the 2008 amendments, FISA allowed unfettered electronic surveillance of communications abroad but restricted the executive branch's power to conduct warrantless electronic surveillance on communications within the United States by requiring that a court find probable cause to believe that the target of the surveillance was an agent of a foreign power.[11] In defense of domestic warrantless wiretapping, the Bush Administration initially argued that it did not violate FISA because a post-September 11 Authorization for Use of Military Force ("AUMF")[12] superseded, or impliedly repealed, existing limitations on electronic surveillance found in FISA.[13] Later, the Bush Administration argued that the post-September 11 AUMF must be construed so as to empower the President, as Commander in Chief, to authorize surveillance without court approval or, at least, to ignore FISA's prohibitions.[14] The Bush

---

available at http://www.nwotruth.com/obama-administration-constitution-does-not-protect-cell-site-records/.

10. Brief for the United States, *supra* note 7.

11. FISA permits domestic electronic surveillance to be initiated before court approval so long as approval is sought within seventy-two hours. It also permits domestic electronic surveillance without court approval during the first fifteen days of a war, and allows for Congress to consider proposals for wartime statutory amendments. *Id.* "FISA is inapplicable to surveillance of communications collected outside the United States and not targeted at U.S. citizens or permanent resident aliens (collectively referred to as "U.S. persons") within the United States. *See* 50 U.S.C. 1801(f)(1)–(2) (defining "electronic surveillance"). Thus, FISA does not impose any limits on wiretapping of calls between foreign nationals outside the United States—whether or not they are associated with al Qaeda—and persons within the United States, as long as the calls are not intercepted domestically, and the tap is not 'targeted' at a U.S. person within the country." Cole & Lederman, *supra* note 4, at 1356 n.5.

12. Authorization for Use of Military Force (AUMF), S.J. Res. 23, 107th Cong. (2001) (enacted).

13. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legal Affairs and U.S. Dep't of Justice, to Sen. Pat Roberts et al., Senate Select Comm. on Intelligence and House Permanent Select Comm. on Intelligence, (Dec. 22, 2005), *reprinted in* 81 IND. L.J. 1360 (2006) [hereinafter DOJ White Paper, Dec. 22, 2005] ("The President stated that these activities are 'crucial to our national security.'").

14. *Id. See also* David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—Framing the Problem, Doctrine, and Original Understanding*, 121 HARV. L. REV. 689, 710 (2008) ("'On the most extreme versions of this view, Congress cannot limit [the President's power to engage in international electronic surveillance] even if it chooses to do so. Foreign surveillance is a presidential prerogative, akin to dictation of the movement of troops . . . .'" (quoting Cass R. Sunstein, *Clear Statement Principles and*

Administration further argued that the TSP was narrowly targeted and therefore all surveillance conducted as part of the TSP would have survived the probable cause standard had it been applied.[15] Essentially, even if the Bush Administration had flouted an act of Congress and circumvented the Foreign Intelligence Surveillance Court, it still had not violated any persons' constitutional rights.[16]

Each of these arguments is post hoc and construed to maximize the power of the executive.[17] The Bush Administration attempted to justify its actions with the sense of exigency that existed post-September 11,[18] but the history of FISA and the clarity of the statute show that Congress intended to prevent precisely the type of surveillance carried out under the TSP. The Supreme Court articulated in *Youngstown Sheet and Tube Co. v. Sawyer*[19] and subsequent cases that the Commander in Chief does not have authority to flout an act of Congress. Furthermore, the TSP violated Fourth Amendment rights Congress originally intended FISA to safeguard. The Supreme Court and Congress had anticipated and intentionally prescribed checks on the executive branch's power for situations of national crisis and threats to national security, such as the September 11 terrorist attack.

National Security: Hamdan and Beyond, 2006 SUP. CT. REV. 1, 38-39 (2006))). *See also* Letter from William E. Moschella, Assistant Attorney Gen., Office of Legal Affairs and U.S. Dep't of Justice, to the Honorable F. James Sensenbrenner, Jr., Chairman of the Comm. on the Judiciary, U.S. House of Representatives, (Mar. 24, 2006) *available at* http://www.fas.org/irp/agency/doj/fisa/doj032406.pdf [hereinafter Letter from Moschella to the Honorable Sensenbrenner (Mar. 24, 2006)], ("The President has inherent constitutional authority over the gathering of foreign intelligence—authority that Congress may not circumscribe.").

15. Letter from Moschella to the Honorable Sensenbrenner (Mar. 24, 2006), *supra* note 14, at 7. Barron & Lederman, *supra* note 14, at 711 n.65.

16. *Id.*

17. Memorandum from U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *reprinted in* 81 IND. L.J. 1375, 1401-02 (2006) [hereinafter DOJ White Paper, Jan. 19, 2006].

18. DOJ White Paper, Dec. 22, 2005, *supra* note 13, at 1363 ("The President stated that these activities are "'crucial to our national security.'"). *See also* Memorandum from John C. Yoo to Alberto R. Gonzales, Counsel for the President, (Oct. 23, 2001), *available at* http://www.salon.com/opinion/greenwald/2009/03/03/yoo/index.html.

19. Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 643-47 (1952) (Jackson, J., concurring).

Courts are presently considering the constitutionality of the TSP,[20] and President Obama is presently under pressure to keep his promise to protect civil liberties.[21] This paper will argue that the potential national security benefits of warrantless domestic wiretapping are insufficient to justify its gross compromise of civil liberties and, moreover, that it was unconstitutional for President Bush to authorize the TSP because he flagrantly abused the power vested in him as Commander in Chief and directly flouted Congressional intent.

I. The Commander in Chief Does Not Have Authority To Flout an Act of Congress

In the days after September 11, instead of going to an amenable Congress to extend his eavesdropping powers, the President decided to exert executive power and authorize the TSP. By doing so, he went beyond his constitutional authority.[22]

The DOJ attempted to justify the President's actions by arguing the overall superintendence of the Commander in Chief: that the Commander in Chief has indefeasible authority to control the conduct of war once it is underway (preclusive of the exercise of Congress's Article I powers) or, in the alternative, that the President has a constitutional duty to respond to an unforeseen attack with whatever means necessary.[23] The DOJ is wrong that the Commander in Chief Clause gives the President preclusive power. Even during wartime, the President is accountable to Congress, and executive actions that violate express or implied statutory limitations are invalid. Furthermore, and contrary to the government's *Youngstown* analysis, the AUMF did not place the President at the height of his authority.

---

20. Glenn Greenwald, *Today's FISA Ruling: A Case Study in 8 Years of Lying and Ignorance*, SALON, Jan. 15, 2009, http://www.salon.com/opinion/greenwald/ 2009/01/15/ fisa/index.html (discussing the FISA Court's ruling on whether the Protect America Act is constitutional under the Fourth Amendment).

21. Glenn Greenwald, *Keith Olbermann's Scathing Criticism of Obama's Secrecy/Immunity Claims*, SALON, Apr. 8, 2009, http://www.salon.com/opinion/greenwald/ 2009/04/08/criticism/index.html; McJoan, *More Immunity Claims on Wiretapping from Obama DOJ*, DAILY KOS, Apr. 7, 2009, http://www.dailykos.com/storyonly/2009/4/7/ 717546/-More-Immunity-Claims-on-Wiretapping-from-Obama-DOJ.

22. *Id.* at 279, 284, 290.

23. DOJ White Paper, Jan. 19, 2006, *supra* note 17. *See also* Barron & Lederman, *supra* note 14, at 694, 704–05, *reprinted in* THE TORTURE PAPERS: THE ROAD TO ABU GHRAIB 13 (Karen J. Greenburg & Joshua A. Dratel eds., 2005)).

A. The Commander in Chief Clause Prescribes Limited Power

The Commander in Chief Clause reads:

> The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States; he may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any subject relating to the Duties of their respective Offices, and he shall have Power to Grant Reprieves and Pardons for Offenses against the United States, except in Cases of Impeachment.[24]

According to the DOJ, any powers granted by Article II, including the Commander in Chief Clause, must also be immune from statutory limitation.[25] FISA, therefore, could not encroach on the President's power. But although the President might enjoy a particular power, it does not mean that statutes cannot temper his exercise of that power.[26]

The historical record is scant and ambiguous as to the degree of power vested in the President through Commander in Chief Clause. While the DOJ argues that the Constitution and the Framers' intent was to vest in the President broad, almost infinite, powers supreme over Congress',[27] there is evidence that the Framers viewed the Commander in Chief's power narrowly.[28] In *The Federalist No. 69*, Hamilton described the Commander in Chief Clause as inferior to that of the British Crown: "It would amount to nothing more than the supreme command and direction of the military . . . while that of the British King extends to the *declaring* of war, and to the *raising and regulating* of fleets and armies."[29] Hamilton's comparison suggests that the power vested in the Commander in Chief to conduct military campaigns is not beyond legislative control.[30]

Scholars Barron and Lederman argue that no post-Founding historical consensus has ever developed among the political branches

---

24. U.S. CONST. art. II, § 2.

25. Barron & Lederman, *supra* note 14, at 741.

26. *Id.* at 742.

27. Memorandum from John C. Yoo to Alberto R. Gonzales, *supra* note 18, at 6.

28. STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 557, at 23 (2007).

29. *Id.* (quoting THE FEDERALIST NO.69, at 418 (Alexander Hamilton) (Clinton Rossiter ed., Penguin Group Inc. 1961) (1788)).

30. Barron & Lederman, *supra* note 14, at 696.

in favor of the Commander in Chief's preclusive power over the conduct of campaigns during wartime.[31] Rather than interpret the Commander in Chief Clause, the Court has grounded its war powers decisions largely in statutory interpretations. In the seminal case regarding statutory limits on the President's war powers of *Little v. Barreme*, the Court considered the liability of Captain Little, who captured a suspected American ship sailing from a French port during "the hostilities between the United States and France."[32] Captain Little had captured the ship according to President Adams' executive order to seize ships sailing or bound *to or from* French ports, but Congress had passed an act only authorizing the Navy to seize American ships that appear to be bound or sailing *to* any port or place within France.[33] The Court held that because the President's order exceeded the authority extended by legislative action, the Captain would face liability.[34] In other words, when Congress has prescribed the manner in which its authorization for the use of armed force is to be executed, its prescription is binding even on the President.[35]

From the time of that decision up to 1950, Congress enacted regulations of the President's authority in every area, and the executive accepted those regulations without constitutional challenge.[36] Contrary to the DOJ's argument, the historical record does not support the idea of preclusive Article II powers for the Commander in Chief; the Commander in Chief is still accountable to Congress and must respect statutory limitations.

Since 1950, Congress has enacted restrictions too often, and Presidents have challenged their legality too infrequently for anything

31. *Id.* at 697.

32. Little v. Barreme, 6 U.S. (2 Cranch) 170, 177 (1804).

33. *Id.* at 170.

34. *Id.* at 179.

35. Because this case is entirely about the President flouting the act of Congress and the language of the executive order as compared to the act of Congress, I reject the reading that this case should be read narrowly regarding the liability of military subordinates or that the Court never reached the question of the President's inherent constitutional authority to go beyond Congress' commands. *See* John. C. Yoo, *The Continuation of Politics By Other Means: The Original Understanding of War Powers*, 84 CAL. L. REV. 167, 294–95 n.584 (1996) (arguing that *Little v. Barreme* did not call upon the United States Supreme Court to settle an inter-branch war dispute, but instead the Court resolved the issue by deferring to Congress' legislative power concerning captures on water).

36. Barron & Lederman, *supra* note 14, at 697.

like a tradition of preclusive power to have taken root. The executive has consistently read statutes in such a way that "interpret[s] away the legislative constraint, leaving it to Congress to respond by attempting to impose (or re-impose) the constraint, but this time with unmistakable clarity."[37]

Meanwhile in 1952, the Supreme Court in *Youngstown* held that even during wartime, the Executive's actions are invalid when they violate express or implied statutory limitations.[38] The Court invalidated the President's seizure of the steel mills during the Korean War because Congress had previously rejected an amendment that "would have authorized such governmental seizures in cases of emergency."[39] The *Youngstown* Court took a restrained view of the President's authority during wartime, contrasting the government's view of the executive with the forefathers' experience with King George III, which surely inspired a negative impression of an all-powerful executive.[40]

Justice Jackson's concurring opinion further articulates the Court's view on the executive branch's interdependence with the other branches. Reading the Commander in Chief Clause against the historical backdrop of the Revolutionary War and the Third Amendment, Justice Jackson rejected the government's argument that the Clause gave the President unchecked military authority:

> Just what authority goes with the name [Commander in Chief] has plagued presidential advisors who would not waive or narrow it by nonassertion yet cannot say where it begins or ends.... Hence, this loose appellation is sometimes advanced as support for any presidential action, internal or external, involving use of force, the idea being that it vests power to do anything, anywhere, that can be done with an army or navy.... [But] [t]here are indications that the Constitution did not contemplate that the title Commander in Chief *of the Army and Navy* will constitute him also Commander in Chief of the country, its industries and its inhabitants. He has no monopoly of 'war powers,' whatever they are.[41]

37. *Id.* at 697, 715–16.

38. *Id.* at 702–03.

39. Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 586 (1952).

40. *Id.* at 641 (Jackson, J., concurring).

41. *Id.* at 641–44 (Jackson, J., concurring).

Justice Jackson further articulated that the President's authority as Commander in Chief was specifically limited in the area of domestic affairs: "That military powers of the Commander in Chief were not to supersede representative government of internal affairs seems obvious from the Constitution and from elementary American history."[42] Moreover, the Court articulated that the system of checks and balances must be upheld whatever the topic and issue at stake:

> Today a kindly President uses the seizure power to effect a wage increase and to keep the steel furnaces in production. Yet tomorrow another President might use the same power to prevent a wage increase, to curb trade-unionists, to regiment labor as oppressively as industry thinks it has been regimented by this seizure.[43]

More recently, in *Hamdi*, the Court reiterated its intent to restrain executive authority, holding:

> We have long since made clear that a state of war is not a blank check for the president when it comes to the rights of the Nation's citizens.... Whatever power the United States Constitution envisions for the Executive in its exchanges with... enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.[44]

Contrary to the DOJ's argument, the Court has not consistently held that the Commander in Chief's powers are immune from statutory limitation: in *Youngstown,* and in *Hamdi*, the Court clearly intended to delineate executive authority in a way that was autonomous, and yet interdependent and reciprocal with the other branches of government.[45] The Court does not always give deference to the Executive. Like the seizure of steel mills at issue in *Youngstown*, the President's authorization of the TSP violates express limitations, and is therefore invalid.

42. *Id.* at 644 (Jackson, J., concurring).

43. *Id.* at 633 (Douglas, J., concurring).

44. Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

45. *See id.* at 536; *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

B. The Commander in Chief Clause Does Not Give the Executive Authority to Conduct Warrantless Domestic Wiretapping During Wartime

In Justice Jackson's famous and widely cited concurring opinion in *Youngstown*, he articulated a measure by which the Court could determine whether the President had authority to act autonomously:

> 1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. . . .
>
> 2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. . . .
>
> 3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb . . . . Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.[46]

The *Youngstown* Court invalidated President Truman's authorization to seize the steel mills because Congress had failed to give the President the authority in question.

Whereas President Truman had acted in the absence of congressional authority, or possibly incompatibly with Congress's *implied* will, President Bush's authorization of the TSP was incompatible with an *express* will of Congress. Congress had expressly prohibited the President from conducting domestic warrantless wiretapping.[47] "And it did so in the strongest way possible, *by making the conduct a crime*."[48] Congress had extensively grappled with the constitutional question in the legislative process and had crafted the statute specifically in order to preclude the

46. *Youngstown*, 343 U.S. at 635–39.

47. *The National Security Agency's Domestic Spying Program: February 2, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department White Paper of January 19, 2006, reprinted in* 81 IND. L.J. 1415, 1419 (2006) [hereinafter *February 2, 2006 Letter from Scholars*].

48. *Id.*

President from invoking a constitutional authority to engage in electronic surveillance outside the means FISA prescribes.[49]

The DOJ attempted to apply *Youngstown* to the TSP, arguing that the President acted at the height of his authority since his actions were in accordance with the AUMF,[50] in spite of the fact that they were in contradiction to FISA, a long-standing, much-deliberated act of Congress. According to the DOJ, "the AUMF place[d] the President at the zenith of his powers" under the tripartite framework of executive authority the Supreme Court set forth in *Youngstown*.[51] Since the AUMF granted broad authorization to the President to act as the Commander in Chief, "the President's power in authorizing the NSA activities [was] at its height because he acted 'pursuant to an express or implied authorization of Congress,' and his power 'include[d] all that he possesses in his own right plus all that Congress can delegate.'"[52] Furthermore, the DOJ argued that the AUMF, as construed by *Hamdi*, authorized the President to "take actions against al Qaeda and related organizations that amount to 'fundamental incident[s] of waging war,' and therefore also authorized the President to conduct warrantless domestic wiretapping, since intercepting enemy communications had long been recognized as a fundamental incident of the use of military force.[53]

The DOJ clearly misapplied *Youngstown*: the DOJ misconstrued the intent and the resulting law from *Youngstown* and is wrong in its assertion that the president acted at the height of his powers. Nothing in the AUMF or in the way that any AUMF has ever been upheld gives the President immunity from violating statutes; the DOJ was overbold and wrong in arguing that the President acted at the height of his authority.[54]

---

49. *Id.*

50. Letter from William E. Moschella, Assistant Attorney Gen., Office of Legislative Affairs, U.S. Dep't of Justice, to Sen. Pat Roberts et al., 1 (Dec. 22, 2005), *reprinted in* 81 IND. L.J. 1360, 1362 (2006).

51. DOJ White Paper, Jan, 19, 2006, *supra* note 17, at 1375 (citing *Youngstown*, 343 U.S. at 635 –39 (Jackson, J., concurring)).

52. *Id.* (citing *Youngstown*, 343 U.S. at 635).

53. *Id.* at 1386 (quoting Hamdi v. Rumsfeld, 542 U.S. 507, 519 (2004) (plurality opinion)).

54. *See* ACLU v. NSA, 493 F.3d 644, 652–53, 716–17 (6th Cir. 2007). Lower courts have held that the DOJ's AUMF and inherent presidential authority arguments are weak. Although the Sixth Circuit Court of Appeals, by a 2-1 decision, vacated a district court order which enjoined the Bush Administration from eavesdropping without warrants, it did so on the basis of standing and did not reach the question of the constitutionality of

II. The AUMF Does Not Authorize Domestic Electronic Surveillance

The statutory language, legislative history, and judicial record make it clear that Congress intended FISA and the criminal code to be the exclusive means by which electronic surveillance is to be conducted.[55] FISA explicitly prohibits surveillance authorized by statute and makes an emergency provision allowing the President to engage in warrantless domestic electronic surveillance for fifteen days immediately following a Congressional declaration of war. The DOJ has read these provisions of FISA extremely narrowly in attempt to argue that the statute permits the President, as Commander in Chief, to generally conduct domestic electronic surveillance without a warrant and obtain Congressional approval post hoc.[56] Furthermore, the DOJ has read Congressional intent very conservatively, proclaiming that although Congress limited executive power to conduct domestic surveillance, Congress did so cautiously and with great deference to the executive branch; "Congress did not attempt through FISA to prohibit the Executive Branch from using electronic surveillance. Instead, Congress acted to bring the exercise of that power under more stringent congressional control."[57] The DOJ minimized a vast legislative history, characterizing FISA as hasty and marginal: "Congress understood it was legislating on fragile constitutional ground and was pressing or even exceeding constitutional limits in regulating the President's authority in the field of foreign intelligence."[58] The DOJ further concluded that since the legislature provided for a modicum of discretion to exercise executive authority to conduct electronic surveillance for a brief period

---

the TSP. In a separate opinion, one of the three judges, Judge Gilman, reiterated the district judge's holding that the TSP program violated FISA, and that enactment of the AUMF did not alter that result. He also held that FISA was constitutional as applied to the TSP and that the President did not have an Article II power to disregard the statute, citing the Jackson concurrence in *Youngstown*, that the President's Commander in Chief authority was at its "lowest ebb" on the issue of domestic warrantless wiretapping. Glenn Greenwald, *Yesterday's Ruling on NSA Warrantless Eavesdropping*, SALON, Jul. 7, 2007, http://www.salon.com/opinion/greenwald/2007/07/07/nsa/; Marty Lederman, *The Sixth Circuit Opinions in the TSP/FISA Case* (Jul. 6, 2007), http://balkin.blogspot.com/2007/07/sixth-circuit-opinion-in-tspfisa-case.html, citing *Youngstown*, 343 U.S. at 635–39.

55. 18 U.S.C. § 2511 (2008). *See also February 2, 2006 Letter from Scholars, supra* note 47, at 1417.

56. DOJ White Paper, Jan. 19, 2006, *supra* note 17, at 1393–94.

57. *Id.* at 1393.

58. *Id.* at 1392.

immediately following declaration of war, the AUMF must have been sufficient to extend that authority indefinitely and in the place of a judicial warrant.[59]

But in contrast to the DOJ's claims, as will be shown below, the history and statutory language of FISA clearly support strong judicial and Congressional intent to limit the authority of the executive to conduct warrantless domestic wiretapping.

A. Courts Explicitly Intended To Limit Executive Power To Wiretap Within the Context of Heightened National Security Concerns.

The national security crisis post-September 11 and the heightened call for surveillance was precisely the type of situation to which the Supreme Court intended for judicial review to apply when it held that warrants were constitutionally required for all domestic surveillance, electronic and otherwise.[60] In 1967, the Supreme Court rejected the government's argument that Fourth Amendment requirements should be relaxed in order to fight organized crime.[61] Shortly thereafter, the exposure of President Nixon's improper use of federal resources to spy on political and activist groups and the government's extensive electronic surveillance against the anti-Vietnam War movement and the Black Power movement led to a court challenge to electronic surveillance conducted for "domestic security" purposes.[62] In *United States v. U.S. Dist. Court (Keith)*, the Court considered the constitutionality of warrantless electronic surveillance of three citizens who were allegedly conspiring to bomb a CIA office in Ann Arbor, Michigan.[63] The Court rejected the government's arguments that un-reviewed surveillance had been

59. *Id.* at 1393–94, 1396.

60. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 312 (1972). *See also* Berger v. New York, 388 U.S. 41, 58–60 (1967) (holding that a New York statute authorizing electronic surveillance violated the Fourth Amendment because: (1) "it did not requir[e] the belief that any particular offense has been or is being committed; nor that the 'property' sought, the conversations, be particularly described"; (2) it failed to limit the duration of the surveillance to impose sufficiently stringent requirements on renewals of the authorization; and (3) the statute "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts"); Camara v. Mun. Court, 387 U.S. 523, 532 (1967) (holding that a warrant was required regardless of the purpose of the search); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that Fourth Amendment's probable cause and warrant requirements apply to electronic surveillance).

61. *Berger*, 388 U.S. at 58–60.

62. *Keith*, 407 U.S. at 299.

63. *Id.*

necessary in light of domestic threats to national security.[64] The Court expressed that in national security crises, that although the investigative duty of the executive may be stronger, there is also greater jeopardy for constitutionally protected speech.[65]

> The danger of political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." ... The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.[66]

Weighing the asserted government need for collecting and maintaining intelligence against Fourth Amendment protections, the Court unanimously held that domestic warrantless surveillance was unconstitutional and concluded that prior warrants would be required for domestic surveillance.[67]

The Court left open the question of foreign intelligence gathering and held warrantless surveillance was constitutional where foreign powers are involved.[68] Following *Keith*, several lower courts held that warrantless foreign electronic surveillance was constitutional, but in 1975, the D.C. Circuit held that warrantless surveillance of the Jewish Defense League ("JDL") was unconstitutional because the JDL was not a foreign power or an agent of a foreign power.[69] The circuit court articulated that its

---

64. *Id.* at 320–21. The Court recognized the executive branch's interest in protecting national security and the value of electronic surveillance in detecting security threats, but nonetheless held that the decision to conduct electronic surveillance cannot be left to the discretion of law enforcement officials. *Id.* The Court rejected the executive branch's arguments that "internal security matters are too subtle and complex for judicial evaluation" and that "prior judicial approval will fracture the secrecy essential to official intelligence gathering." *Id.* The Court also rejected the executive branch's argument that exceptions to the Fourth Amendment warrant requirement should be recognized for domestic security surveillance. *Id.*

65. *Id.* at 314, 317.

66. *Id.* at 314.

67. *Id.* at 322–24.

68. *Id.* at 321–22.

69. William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099, 1110 (2007) (citing Zweibon v. Mitchell, 516 F.2d 594, 614 (D.C. Cir. 1975) (en banc) ("[A] warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power, even if the surveillance is installed

decision was in no way meant to restrict legitimate surveillance of organizations that posed a threat to the United States, and that the determination of necessity must be made by a neutral, disinterested magistrate or judge—not by an executive official with investigative and prosecutorial interests.[70]

The Court articulated the need to uphold Fourth Amendment protections for electronic surveillance in response to a political climate and executive arguments very similar to national security interests post-September 11.[71] The judiciary was clear that even in a climate of threats to national security, the Fourth Amendment required an independent oversight of the executive's intelligence gathering.

B. Congress Explicitly Intended To Limit Executive Power To Wiretap Within the Context of Heightened National Security Concerns.

The Court's holding in *Keith* that Fourth Amendment protections must apply to electronic surveillance formed the basis for Congress to draft and pass the Foreign Intelligence Surveillance Act a few years later.[72] In *Keith*, the Supreme Court rejected the government's argument that surveillance conducted without prior judicial approval was a lawful and reasonable exercise of the President's power to protect national security.[73] The Court held "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the

---

under presidential directive in the name of foreign intelligence gathering for protection of the national security. . . . [O]ur decision does not limit in any way the ability of the President to conduct legitimate national security wiretaps, since we do not address the substantive scope of that power or the exact standards upon which warrants should issue. Rather, we merely decide that whatever the legitimate scope of [executive branch] power, and whatever the standard which must be met to justify the intrusion of a wiretap, the decision as to whether the scope has been exceeded or the standard has been met is to be made by a neutral and disinterested magistrate or judge rather than by an Executive official engaged in investigatory or prosecutorial duties, at least in situations where the subject of the surveillance is a domestic organization that is not the agent of or acting in collaboration with a foreign power.")).

70. *Zweibon*, 516 F.2d at 614.

71. Mayfield v. United States, 504 F. Supp. 2d 1023, 1038 (D. Or. 2007).

72. Cole & Lederman, *supra* note 4, at 1355.

73. *Keith*, 407 U.S. at 301, 314, 312–13 ("There is understandably, a deep-seated uneasiness and apprehension that this [electronic surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.").

discretion of the Executive Branch," and required the executive branch to make application to a federal judge and show probable cause before conducting domestic electronic surveillance.[74]

Four years after *Keith*, a Senate Committee on intelligence activities, known as the Church Committee, detailed widespread warrantless surveillance, including politically motivated intelligence files kept by the CIA, the FBI, the United States Army, and the Internal Revenue Service.[75] Under public pressure to respond to and prevent future excesses of government surveillance, Congress passed the Foreign Intelligence Surveillance Act in 1978. While the Court circumscribed the executive branch's power to conduct warrantless surveillance, the press exposed further intelligence agency abuses, including NSA surveillance of Americans and drug traffickers, U.S. Army military intelligence surveillance of domestic groups, and CIA opening of domestic mail sent to or received from abroad, all of which increased public pressure on Congress.[76] Meanwhile, the executive branch sought to preserve its powers to conduct surveillance, and so for the first time it seemed possible that a bill regarding electronic surveillance for foreign intelligence purposes

74. *Id.* at 316–17.

75. United States Senate Select Comm. to Study Gov't Operations with Respect to Intelligence Activities, *Final Report of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, Book 2: Intelligence Activities and the Rights of Americans*, S. REP. NO. 94-755, pt. 2, at 6–7 (1976). The Church Committee detailed some of the revelations of illegal spying and other activities by U.S. intelligence agencies.

> FBI headquarters alone has developed over 500,000 domestic intelligence files, and these have been augmented by additional files at FBI Field Offices. The FBI opened 65,000 of these domestic intelligence files in 1972 alone. . . . The number of Americans and domestic groups caught in the domestic intelligence net is further illustrated by the following statistics: Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953-1973, producing a CIA computerized index of nearly one and one-half million names. . . . Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA Operation CHAOS (1967-1973). . . . An estimated 100,000 Americans were the subject of United States Army intelligence files created between the mid-1960's and 1971. Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria. At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a 'national emergency.'

Id.

76. William Funk, *supra* note 69, at 1110.

could overcome presidential veto.[77] Senator Edward Kennedy and Attorney General Edward Levi created FISA as a middle path.[78]

FISA prescribed procedures for physical and electronic surveillance and the collection of foreign intelligence information where the Fourth Amendment had previously provided very general limitations.[79] FISA limited government surveillance to phone calls (and subsequently e-mail communications) on foreign soil or coming into the United States.[80] The NSA could target phone and email messages within the United States only if the NSA first obtained a court order from the specially established FISC, which holds closed sessions at the Justice Department.[81]

Congress intended, and FISA spelled out, that a court order must be required for any domestic electronic surveillance. An application for a judicial order certifying electronic surveillance of a foreign power or agent of a foreign power must "certify that the purpose of the surveillance is to obtain foreign intelligence information."[82] Congress explained that the intent behind this requirement was "to prevent the practice of targeting one individual for electronic surveillance when the true purpose of surveillance is to gather

77. *Id.* at 1111.

78. As passed, FISA authorized electronic surveillance of a foreign power or agent of a foreign power to obtain intelligence information if either (1) the Attorney General certified under oath that the surveillance was solely directed at communications transmitted exclusively between certain "foreign powers" and the surveillance was one that was not intended to and was unlikely to obtain communications of a "United States person," in which case the Attorney General could authorize surveillance for up to one year; or (2) the Attorney General submitted an application to the FISC containing information about the identity, place, and justification for surveillance, and specifically certifying that the purpose was for intelligence gathering, that information sough is foreign intelligence information, and that the information could not reasonably be obtained through normal means. *Id.* at 1112–15.

79. The Communications Act of 1934, 47 U.S.C. §§ 151–614 (2008), imposed the first obstacles to electronic surveillance, making it a crime for any person to "intercept any communication and divulge or publish the . . . contents" of wire and radio communications. 47 U.S.C. § 605 (2008). Prior to 1967, electronic surveillance by itself was not considered a "'search"' under the Fourth Amendment because such surveillance was conducted merely for intelligence purposes. The Supreme Court had interpreted this provision as applying to the government and consequently held that evidence so obtained was not admissible in court but permitted intelligences surveillance to continue so long as the contents were not divulged nor published. Funk, *supra* note 69, at 1103–04. *See also* DONALD J. MUSCH, CIVIL LIBERTIES AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 157, 7 (2003).

80. Funk, *supra* note 69 at 1113–14.

81. 50 U.S.C. 1801(f)(1)–(2); *see also* James Risen & Eric Lichtblau, *supra* note 2.

82. Funk, *supra* note 69, at 1115.

information about another individual . . . and to make explicit that the sole purpose of such surveillance is to secure foreign intelligence information and not to obtain information for any other purpose."[83]

Through FISA, Congress restrained the power of the executive to gather information in a dragnet fashion as a means for initiating criminal prosecutions. Traditionally, intelligence operations undertaken by the CIA and military intelligence agencies simply to obtain information on the intentions, capabilities, and activities of those able to harm the United States, are separated from gathering information usually unrelated to criminal activity that might be prosecuted.[84] In passing FISA, Congress recognized the distinction between intelligence gathering and criminal prosecutions, but in no way attempted to create a barrier to sharing information.[85] One of the drafters of the original FISA, William Funk, writes, "It is clear that this language was never intended to preclude the dissemination and use of foreign intelligence information for law enforcement purposes, so long as the purpose of the surveillance was to acquire foreign intelligence information."[86]

Nevertheless, during the 1990s, the Department of Justice Office of Intelligence Policy and Review and later the FISC itself instituted rules effectively cutting off communications between FBI intelligence personnel and the Criminal Division.[87] This misconception—or misrepresentation—about FISA's limitations led to efforts to circumvent and reform FISA post-September 11, 2001.[88] As originally intended, FISA placed little constraint on consultation and coordination between agencies and no limitation on the use of information in criminal trials; but multiple presidential administrations—especially the Bush Administration—interpreted FISA as imposing limitations and used that as justification to convince Congress and the public that security was compromised as a result.[89]

The legislative history of FISA expressly declares Congress's intent for FISA to be the exclusive source of executive branch power

83. *Id.* at 1116.
84. *Id.* at 1104.
85. *Id.* at 1106.
86. *Id.* at 1116.
87. *Id.* at 1126.
88. *Id.* at 1099.
89. *Id.* at 1138.

to conduct electronic surveillance for foreign intelligence information, and for the executive branch's power to be checked by the judiciary.[90] Congress clearly intended FISA to apply even during wartime and explicitly limited the President's authority to authorize electronic surveillance without a court order to a period not to exceed fifteen calendar days following a declaration of war by Congress.[91]

Courts have continued to hold that when Congress passed FISA, Congress intended strong protections from warrantless domestic wiretapping.[92] In 2008, a district court held:

> The impetus for the enactment of FISA was Congressional concern about warrantless wiretapping of United States citizens conducted under a justification of inherent presidential authority under Article II. Congress squarely challenged and explicitly sought to prohibit warrantless wiretapping by the

90. H.R. REP. NO. 95-1283, pt. 1, at 24 (1978) ("Even if the President has the inherent authority in the absence of legislation to authorize warrantless electronic surveillance for foreign intelligence purposes, Congress has the power to regulate the conduct of such surveillance by legislating a reasonable procedure, which then becomes the exclusive means by which such surveillance may be conducted."); *see also* H.R. REP. NO. 95-1283, pt. 2, at 101 (1978) ("Despite any inherent power of the President to authorize warrantless electronic surveillances in the absence of legislation, by this bill [and Title III] . . . , Congress will have legislated with regard to electronic surveillance in the United States, that legislation with its procedures and safeguards prohibit the President, notwithstanding any inherent powers, from violating the terms of that legislation.").

91. 50 U.S.C. § 1811 (2008).

92. *In re* NSA Telecomms. Records Litig., 564 F. Supp. 2d 1109, 1122–23 (N.D. Cal. 2008) ("In the case of FISA, Congress attempted not only to put a stop to warrantless wiretapping by the executive branch but also to establish checks and balances involving other branches of government in anticipation of efforts by future, administrations to undertake warrantless surveillance in some other manner: 'In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties. This committee is well aware of the substantial safeguards respecting foreign intelligence electronic surveillance currently embodied in classified Attorney General procedures, but this committee is also aware that over the past thirty years there have been significant changes in internal executive branch procedures, and there is ample precedent for later administrations or even the same administration loosening previous standards.' Given the possibility that the executive branch might again engage in warrantless surveillance and then assert national security secrecy in order to mask its conduct, Congress intended for the executive branch to relinquish its near-total control over whether the fact of unlawful surveillance could be protected as a secret." (quoting H.R. REP. NO. 95-1283, pt. 1, at 21 (1978))). *See also* Mayfield v. United States, 504 F. Supp. 2d 1023, 1038 (D. Or. 2007) (on appeal).

> executive branch by means of FISA, as FISA's legislative history amply documented.[93]

The fact that post-September 11, 2001, was precisely the type of situation *Keith* contemplated and which prompted Congress to pass limits on domestic surveillance makes the TSP a complete flouting of Congress's authority and its purpose behind FISA.

C. The Authorization for Use of Military Force Could Not Have Impliedly Repealed Strong Legislative and Judicial Intent

The government's argument that a post-September 11 AUMF impliedly repealed existing limitations on electronic surveillance found in FISA[94] flies in the face of a clearly written statute and this strong judicial and legislative history. As recently as 2006, the Department of Justice argued:

> In the specific context of the current armed conflict with al Qaeda and related terrorist organizations, Congress by statute has confirmed and supplemented the President's recognized authority under Article II of the Constitution to conduct such warrantless surveillance to prevent further catastrophic attacks on the homeland. In its first legislative response to the terrorist attacks of September 11th, Congress authorized the President

---

93. *In re NSA Telecomms. Records Litig.*, 564 F. Supp. 2d at 1122 (holding that the court must recognize Congress' intent for judicial review to apply to the executive). This result is distinguished from *Franklin v Massachusetts*, 505 U.S. 788, 800–01 (1992) where the Court held that the Office of the President was not an executive "agency" whose actions were subject to judicial review under the Administrative Procedures Act.

94. David Cole & Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Legal Authorities Supporting the Activities of the National Security Agency Described by the President, reprinted in* 81 IND. L.J. 1374, at 1409 n.21 (2005). *See also* Cole & Lederman, *supra* note 4, at 1358 n.11. "The *Times* report was based on leaks of classified information, presumably by NSA officials concerned about the legality of the program. The *Times* reported that at the President's request it had delayed publication of the story for more than a year." *Id.* at 1355. Following the *New York Times* story, in December of 2005, the Administration set forth its legal defense of the NSA program in a letter from the Department of Justice (DOJ) addressed to the leaders of the Senate and House Intelligence Committees; "Most prominently, DOJ argued that Congress had implicitly authorized the NSA's warrantless surveillance program when it authorized the use of military force against al Qaeda in September 2001. More obliquely, the DOJ suggested that to interpret the 2001 force authorization statute as *not* authorizing the NSA program would raise a serious constitutional question, because in that case FISA's prohibition of the surveillance would interfere with the President's authority as commander in chief to execute the war against al Qaeda in the manner he thought most effective. Finally, the letter argued that the wiretapping program does not violate the Fourth Amendment." *Id.* at 1357.

> to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th in order to prevent "any future acts of international terrorism against the United States." History conclusively demonstrates that warrantless communications intelligence targeted at the enemy in time of armed conflict is a traditional and fundamental incident of the use of military force authorized by the AUMF.[95]

In making the argument that the AUMF implicitly authorized the executive to circumvent FISA, the DOJ relied on the then-recently issued Supreme Court decision *Hamdi v. Rumsfeld*.[96] The DOJ argued that since the Court had ruled in *Hamdi* that the AUMF gave Congress's express approval to the President to use all traditional and accepted incidents of force in the current military conflict, including detaining American citizens captured on the battlefield in Afghanistan, it also gave its approval to the executive to use warrantless electronic surveillance to intercept enemy communications both at home and abroad.[97]

A number of scholars and former government officials responded that the AUMF could not reasonably be construed to implicitly authorize warrantless electronic surveillance in the United States during wartime because of the existence of FISA.[98] "The DOJ . . . continues to place primary reliance on an argument that the AUMF silently authorized what Congress had in FISA clearly and specifically forbidden—unlimited warrantless wiretapping during wartime."[99] In contrast to the situation considered in *Hamdi*, legislation exists on this exact point: FISA expressly limits authorization for warrantless surveillance to the first fifteen days after war has been declared.[100] Since an AUMF is not even as formal as a declaration of war, which would only authorize fifteen days of

95. Cole & Lederman, *supra* note 94, at 1374–75 (DOJ statement on January 19, 2006, quoting Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C. § 1541 (2008)).

96. Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

97. Cole & Lederman, *supra* note 94, at 1375.

98. David Cole & Martin S. Lederman, *The National Security Agency's Domestic Spying Program: January 9, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005*, 81 IND. LJ. 1364, 1364 (2005); *February 2, 2006 Letter from Scholars*, *supra* note 47, at1415.

99. *February 2, 2006 Letter from Scholars*, *supra* note 47,at 1416.

100. 50 U.S.C. § 1811 (2008).

warrantless wiretapping, to conclude that the AUMF provides the President with *unlimited and indefinite* warrantless wiretapping authority is entirely unreasonable.[101]

In addition, the scholars argued, to interpret the AUMF as implicitly amending FISA would be "a momentous statutory development, undoubtedly subject to serious legislative debate . . . not the sort of thing Congress would enact *inadvertently*."[102] 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."[103]

A critical difference between unlimited warrantless wiretapping and *Hamdi* is that Congress had not specifically regulated detention of American citizens during wartime, whereas electronic surveillance targeting U.S. persons within the United States is the precise conduct regulated by FISA.[104] The DOJ's reading would require interpreting a statute that is entirely silent on the subject to have implicitly repealed and wholly overridden the carefully constructed and criminally enforced "'exclusive means'" created by Congress for the regulation of electronic surveillance.[105]

The Court's holding two years later in *Hamdan v. Rumsfeld* further refutes the DOJ's arguments that the AUMF authorized warrantless wiretapping.[106] In *Hamdan*, the Court held that the military commissions the President established in 2001 transgressed two statutory restrictions that Congress had enacted, Articles 21 and 36 of the Uniform Code of Military Justice ("UCMJ"), which required that military commissions comply with the international laws of war and follow the rules applicable to courts-martial.[107] The Court rejected the argument that the AUMF implicitly authorized the President to implement military commissions where the UCMJ

101. Cole & Lederman, *supra* note 122, at 1416.

102. *Id.*

103. *Id.* (citing Gonzales v. Oregon, 126 S. Ct. 904, 921 (2006) (quoting Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 468 (2001)).

104. *Id.* (citing 50 U.S.C. § 1811).

105. *Id.* at 1416.

106. Curtis A. Bradley et al., Letter to Members of Congress, July 14, 2006, at 2, *available at:* http://www.law.duke.edu/publiclaw/pdf/lettertocongress7-14.pdf (in response to Letter from William E. Moschella, Assistant Att'y Gen., U.S. Dep't of Justice, to Sen. Charles Schumer (July 10, 2006), *available at* http://lawculture.blogs.com/ lawculture/files/ NSA.Hamdan.response.schumer.pdf (arguing that *Hamdan* does not apply)).

107. Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2786, 2790–93, 2804–08 (2006).

specifically provided procedures for establishment.[108] The Court held that "[r]epeals by implication are not favored"[109] and explained in a footnote that even where Congress has declared war, the President is not authorized to do what pre-existing statutes forbid.[110] As with the military commissions in *Hamdan*, nothing in the text or legislative history of the AUMF suggests that Congress intended to expand or alter the authorization of wiretapping set forth in FISA.[111]

Furthermore, FISA's limitations on electronic surveillance are "crystal clear, and uncontroverted."[112] As Suzanne Spaulding, former assistant general counsel at the CIA, articulated,

> The law clearly states that the criminal wiretap statute and FISA are 'the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted.' If these authorities are exclusive, there is no other legal authority that can authorize warrantless surveillance.[113]

The DOJ's argument that the AUMF implicitly repealed a Congressional statute specifically on point is simply preposterous.

A recent account of the Bush Administration suggests that the DOJ's argument that the AUMF implicitly repealed existing limitations on electronic surveillance was entirely post hoc and calculated to maximize executive power.[114] According to U.S. District Judge Royce C. Lamberth, chief of the federal government's special surveillance court when the warrantless eavesdropping began, the Bush administration had no interest in changing the law through constitutional channels: "We could have gone to Congress, hat in

---

108. *Id.*

109. *Id.* at 2775 (citing *Ex parte* Yerger, 75 U.S. (8 Wall.) 85, 105 (1869)).

110. Bradley, *supra* note 106, at 3 (citing *Hamdan,* 126 S. Ct. 2775 n.24).

111. *Id.* at 4.

112. *Id.*

113. Suzanne Spaulding, *Power Play: Did Bush Roll Past the Legal Stop Signs?* WASH. POST, Dec. 25, 2005, at B1, *available at* http://balkin.blogspot.com/2005/12/if-youre-going-to-read-only-one-thing.html (Spaulding is former assistant general counsel at the CIA, general counsel for the Senate and House Intelligence committees, and executive director of the National Terrorism Commission (1999-2000)).

114. Barton Gellman, *Cheney Shielded Bush From Crisis*, WASH. POST, Sept.15, 2008; at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/14/AR2008091401974.html. *See also* JAMES BAMFORD, THE SHADOW FACTORY, THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 110 (2008), at 112–18; GLENN GREENWALD, A TRAGIC LEGACY 93 (2007), at 93–94.

hand, the judicial branch and the executive together, and gotten any statutory change we wanted in those days, I felt like. But they wanted to demonstrate that the president's power was supreme."[115]

In summary, the history and statutory language of FISA clearly limit executive authority to conduct warrantless domestic wiretapping and to argue that a general AUMF overrides specific provisions in FISA completely perverts congressional intent.

III. The Terrorist Surveillance Program Violated Fourth Amendment Rights

The TSP not only contravened FISA and the separation of powers, but also violated the Fourth Amendment.[116] On March 2, 2009, the DOJ released an Office of Legal Counsel memo October 23, 2001, in which the Bush Administration concluded that "the Fourth Amendment does not apply to domestic military operations," including "intercepting electronic or wireless communications" by "employing surveillance methods more powerful and sophisticated than those available to law enforcement agencies."[117] This flies in the face of the Constitution and the Supreme Court. The Supreme Court has never upheld warrantless domestic wiretapping for any purpose and has struck it down many times.[118]

Another view is that following September 11, the Bush Administration believed that FISA required government officials to certify that the sole or primary purpose of surveillance was to obtain foreign intelligence, rather than obtain evidence for use in a criminal enforcement action.[119] On this basis, the Administration pushed for an amendment to this provision in the USA Patriot Act with the intent of establishing FISA surveillance for use in a possible criminal prosecution so long as some residual foreign intelligence purpose of

115. *See* Gellman, *supra* note 114.

116. *See February 2, 2006 Letter from Scholars*, *supra* note 47, at 1422.

117. *See* Authority for Use of Military Force to Combat Terrorist Activities Within the United States, Op. Off. Legal Counsel 1, 4, 18, (2001), *available at* http://www.eff.org/deeplinks/2009/03/doj-releases-bush-era-olc-memos.

118. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 312 (1972); Berger v. New York, 388 U.S. 41, 58–60 (1967) (holding that a New York statute authorizing electronic surveillance violated the Fourth Amendment); Camara v. Mun. Court, 387 U.S. 523, 532 (1967) (holding that a warrant was required regardless of the purpose of the search); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that Fourth Amendment's probable cause and warrant requirements apply to electronic surveillance).

119. Funk, *supra* note 69, at 1100–02.

the surveillance also existed.[120] The Patriot Act amendment to the purpose requirement tended in the same direction as the TSP—it reduced oversight and gave the government great latitude in gathering domestic information—although it did not go as far as the TSP.

A district court recently held in the *Mayfield v. United States* case that FISA as amended by the Patriot Act violates Fourth Amendment protections,[121] suggesting that the far more egregious TSP might also be found unconstitutional. In *Mayfield*, the court examined claims by plaintiffs who alleged unlawful searches and seizures, and unlawful arrest and imprisonment, after the FBI concocted false and misleading affidavits in order to justify intrusive searches and Brandon Mayfield's arrest as a material witness in the Madrid commuter train bombings of 2004.[122] The district court held that the Patriot Act FISA amendments are unconstitutional because they permit the government to perform covert physical searches and electronic surveillance and wiretaps of the home, office and vehicles of a person without first requiring the government to demonstrate to a court (1) the existence of probable cause and (2) that the primary purpose of the searches and surveillance is to obtain foreign intelligence information.[123] In other words, the Patriot Act effectively eliminates the probable cause requirement that FISA previously relaxed only for national security intelligence gathering, allowing the executive branch to bypass the Fourth Amendment in gathering evidence for a criminal prosecution.[124] The district court held that *Keith* should remain the guiding principle: the decision to conduct electronic surveillance cannot be left to the discretion of law enforcement officials.[125]

120. 50 U.S.C. § 1804(a)(6)(B) (2008); Funk, *supra* note 69, at 1101 ("The immediate aftermath of September 11, 2001 . . . was not the best situation in which to consider calmly either the necessity or all the ramifications of a change to the purpose requirement. . . . FISA now constitutes a system by which the government can intentionally subject a person to the most wide-ranging and intrusive searches to obtain evidence of criminal behavior for the purposes of using it in a criminal prosecution, absent the traditional safeguards associated with searches for evidence of crimes.").

121. Mayfield v. United States, 504 F. Supp. 2d 1023, 1039 (D. Or. 2007) (on appeal).

122. *Id.*

123. *Id.* at 1032.

124. *Id.* at 1037.

125. *Id.* at 1038.

So far, *Mayfield* stands alone and against other district courts upholding the constitutionality of recent FISA amendments,[126] but whether the TSP violated Fourth Amendment protections is still an open question,[127] for in most cases plaintiffs have been denied standing.[128]

IV. Warrantless Domestic Wiretapping Fails To Achieve Substantial Benefits to National Security

Not only was the TSP an unconstitutional executive act that violates the public's Fourth Amendment rights, it also failed to resolve intelligence problems. The conventional wisdom after September 11, 2001, was that U.S. national security agencies failed to "connect the dots" before the attacks.[129] In contrast, others saw a more critical intelligence failure that there were "too few useful dots."[130] By circumventing FISA, however, the TSP solved neither of these institutional problems.

The government defends the TSP with the argument that FISA impeded intelligence work by creating a "wall" that restricted the degree of cooperation between law enforcement and intelligence collectors and limited the use of information in criminal prosecutions.[131] Neither of these arguments explain the government's failure to intervene in the September 11 terrorist attacks when the NSA had conducted judicially authorized electronic surveillance since 1999 on two September 11 terrorists, Khalid al-Mihdhar and Nawaf al-Hazmi, and had shared their identities with the CIA and FBI.[132]

---

126. *See* United States v. Abu-Jihaad, 531 F. Supp. 2d 299 (D. Conn. 2008); United States v. Warsame, 547 F. Supp. 2d 982 (D. Minn. 2008); United States v. Mubayyid, 521 F. Supp. 2d 125 (D. Mass. 2007) (holding that FISA does not violate the Fourth Amendment's judicial review, probable cause, particularity, and notice requirements).

127. Greenwald, *supra* note 20.

128. *In re NSA Telcomms. Records Litigation* is the only pending case. On January 5, 2009, plaintiffs survived the government's motion to dismiss for lack of standing. *In re* NSA Telcomms. Records Litig., 595 F. Supp. 2d 1077 (N.D. Cal. 2009) (appeal denied). *See also* ACLU v. NSA, 493 F.3d 644, 652–53 (6th Cir. 2007); David Krayets, *Appeals Court Allows Classified Evidence in Spy Case*, WIRED BLOG NETWORK, February 27, 2009, http://blog.wired.com/27bstroke6/2009/02/appeals-court-a.html.

129. DYCUS, *supra* note 28 (quoting Robert Bryant et al., *America Needs More Spies*, ECONOMIST, July 12, 2003, at 30).

130. *Id.*

131. MUSCH, *supra* note 79,

132. *Democracy Now!: James Bamford: The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (Democracynow.org Internet broadcast Oct.

Eliminating the requirement for court approval of electronic surveillance would have done nothing to improve intelligence efforts related to the September 11 terrorist attacks.[133]

The government's argument that FISA impeded effective intelligence gathering is equally implausible. Passed in 1978, the Foreign Intelligence Surveillance Act created a separate, secret court, the Foreign Intelligence Surveillance Court ("FISC"), to consider warrant requests and ostensibly ensure a check on the activities of the executive branch.[134] All of the FISC's opinions and Justice Department guidance documents are kept secret: The government is not required to disclose the number of U.S. citizens who are subjected to each type of FISA surveillance, where surveillance occurred, the average length of surveillance and extensions, or the number of targets subsequently arrested and convicted.[135] Regarding clandestine physical searches, the government need not show any special need for secrecy or give any notice; FISA permits secrecy that the Fourth Amendment clearly prohibits outside the intelligence-gathering context.[136]

The FISC has given virtually universal approval to the large number of government requests for electronic surveillance: From 1997-2002, the government made between 749 and 1,228 applications for electronic surveillance each year.[137] The FISC approved every single one.[138] After September 11, Congress passed the Patriot Act, increasing the government's authority to collect and share wiretap information between agencies and authorizing surveillance where the purpose was not exclusively to gather foreign intelligence information.[139] With the passage of the Patriot Act, government use of FISA warrants exploded.[140] In short, before and after September

14, 2008), http://www.democracynow.org/2008/10/14/james_bamford_the_shadow_factory_the.

133. GREENWALD, *supra* note 114.

134. MUSCH, *supra* note 79, at vii.

135. STEPHEN J. SCHULHOFER, RETHINKING THE PATRIOT ACT: KEEPING AMERICA SAFE AND FREE 50 (2005).

136. *Id.* at 52.

137. MUSCH, *supra* note 79, at vii.

138. *Id.*

139. *Id.* at 205. *See also* ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 2, 57 (2002).

140. SCHULHOFER, *supra* note 135, at 43. *See also* DYCUS, *supra* note 28, at 547 (In 2003, the FISC approved 1,724 warrants that represented an 85 percent increase from 2002, denied four, and made substantive modifications in seventy-nine others. In 2005, the

11, 2001, the FISC allowed the President to do almost any eavesdropping he wanted: the warrant requirement did not impede effective or efficient intelligence gathering.[141] Moreover, if the executive found FISA to be impeding intelligence gathering, the President could have gone to a very accommodating Congress to amend the law to extend to the executive even greater eavesdropping powers.[142]

In addition to FISA not being restrictive enough to warrant unlimited electronic surveillance, there is no clear basis that mass electronic surveillance results in the production of substantive intelligence and, specifically, has produced any tangible results in the war on terrorism.[143] After the NSA began conducting warrantless wiretapping, what the agency gained in speed and freedom, it sacrificed in order and understanding.[144] In addition, of all the terrorist prosecutions since September 11, the vast majority were charged with "material support" to a group the government has labeled terrorist under a very broad statute; the government has obtained a number of convictions or guilty pleas, but none of the defendants have been charged with engaging in terrorist activity.[145] The only criminal conviction involving an actual terrorist incident since September 11 was that of shoe bomber Richard Reid, captured simply because an alert airline employee noticed him trying to light his shoe on fire.[146] Dragnet surveillance has failed to detect a terrorist cell within the United States.[147] The results of electronic surveillance are largely unknowable given its secret nature;[148] but as far as the public knows, warrantless domestic electronic surveillance has failed to yield "useful dots"—substantive intelligence—or help the

government made 2,074 applications to the FISC, the government withdrew two applications prior to a FISC ruling, and the FISC approved 2,072 applications.). Additionally, for brief annual FISA reports, see http://www.usdoj.gov/oipr/readingroom/2005fisa-ltr.pdf.

141. BAMFORD, *supra* note 114, at 110.

142. Greenwald, *supra* note 21. *See also* BAMFORD, *supra* note 114, at 300.

143. DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY 232 (2006). *See also* BAMFORD, *supra* note 114, at 121–23.

144. BAMFORD, *supra* note 114, at 122.

145. *Id.* at 233.

146. *Id.* at 234.

147. *Id.*

148. *Id.*

government "connect the dots," while the risk to civil liberties is enormous.

Extensive electronic surveillance produces a vast quantity of information[149] and substantial risk of misuse of information. The potential for abuse in the digital age far exceeds anything that was possible in the era of paper records.[150] In Germany, constitutional amendments passed in 1968 empowered the federal government to bypass the court system and allow for the surveillance of the mail and telecommunications when national security was said to be at issue.[151] The information gathered was used by both the government and large companies to block the hiring of anyone who had demonstrated support for the radical left opposition as well as to initiate criminal investigations designed to target dissent; by the 1980s, the practice of electronic surveillance was said to have impacted as much as five percent of the West German adult population[152] and probably had an untold impact on chilling legal dissident behavior. Regarding the ongoing collection and electronic storage of information gathered through mass electronic surveillance here in the United States, National Security Agency expert James Bamford says, "it isn't just the picking up of these conversations and listening to them and laughing about them. These conversations are transcribed.... and then they're recorded, and they're kept forever" in an enormous warehouse in Texas.[153] Once the NSA has the information, there is no telling what the government will do with it.[154]

Conclusion

In conclusion, the TSP, and warrantless wiretapping in general, fail to produce substantial benefit to intelligence work and egregiously violate civil liberties. President Bush's authorization of

149. *Id.* at 322, 329, 340 ("With its secret intercept rooms, its sprawling data farms, and its race for exaflop speeds, the NSA is akin to Jorge Luis Borges's 'Library of Babel,' a place where the collection of information is both infinite and at the same time monstrous, where the entire world's knowledge is stored, but not a single word understood.").

150. COLE & DEMPSEY, *supra* note 143, at 230. *See also* BAMFORD, *supra* note 114.

151. JAMES BECKMAN, COMPARATIVE LEGAL APPROACHES TO HOMELAND SECURITY AND ANTI-TERRORIMS 94 (2007).

152. *Id.*

153. BAMFORD, *supra* note 114.

154. Presently, in addition to tracking where people are and what they are doing, Bamford says that the NSA is "developing an artificial intelligence system designed to figure out what people are thinking." *Id.* at 325.

warrantless domestic wiretapping was invalid because the Commander in Chief Clause did not give him authority to contravene a legislative act; and furthermore, warrantless wiretapping is outside the scope of actions fundamental to the incident of waging war. President Obama's continued defense of warrantless wiretapping is, similarly, an illegitimate exercise of executive power. The history and statutory language of FISA clearly limit executive authority to conduct warrantless domestic wiretapping: Warrantless eavesdropping is a criminal offense—a felony. The AUMF cannot be read to impliedly repeal FISA, and to read the AUMF otherwise completely perverts congressional and judicial intent. As the Supreme Court held in *Keith* and as Congress legislated in FISA, the decision to conduct electronic surveillance must not be left to the discretion of law enforcement officials—to do so violates the Fourth Amendment and eviscerates the separation of powers doctrine.

***