

University of Florida Levin College of Law

UF Law Scholarship Repository

UF Law Faculty Publications

Faculty Scholarship

12-2006

Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law

Fletcher N. Baldwin Jr.

University of Florida Levin College of Law, baldwinfn@law.ufl.edu

Robert B. Shaw

Follow this and additional works at: <https://scholarship.law.ufl.edu/facultypub>



Part of the [Constitutional Law Commons](#), [Fourth Amendment Commons](#), and the [National Security Law Commons](#)

Recommended Citation

Fletcher N. Baldwin, Jr. & Robert B. Shaw, *Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law*, 17 U. Fla. J.L. & Pub. Pol'y 429 (2006).

This Article is brought to you for free and open access by the Faculty Scholarship at UF Law Scholarship Repository. It has been accepted for inclusion in UF Law Faculty Publications by an authorized administrator of UF Law Scholarship Repository. For more information, please contact rachel@law.ufl.edu.

DOWN TO THE WIRE: ASSESSING THE CONSTITUTIONALITY OF THE NATIONAL SECURITY AGENCY'S WARRANTLESS WIRETAPPING PROGRAM: EXIT THE RULE OF LAW

Fletcher N. Baldwin, Jr. & Robert B. Shaw***

I.	INTRODUCTION	430
II.	WIRETAPPING—THE GENESIS	435
	A. <i>Origins</i>	435
	1. <i>Olmstead v. United States</i>	435
	2. <i>Nardone v. United States</i>	437
	3. <i>Katz v. United States</i>	438
	B. <i>Keith and the Legality of Wiretapping for Domestic Threats to National Security</i>	440
	C. <i>Attempts to Extend the Keith Doctrine to Foreign Threats</i>	442
	D. <i>The Legislative Response: FISA</i>	444
	E. <i>September 11th and the Genesis of the NSA Program</i> ...	447
II.	THE PRESIDENT LACKS BOTH THE CONGRESSIONAL AUTHORIZATION AND INHERENT AUTHORITY TO EFFECTUATE THE NSA PROGRAM	449
	A. <i>The President Lacks Congressional Authority to Effectuate the NSA Program</i>	450
	B. <i>The President Lacks the Inherent Authority to Effectuate the NSA Program</i>	456
III.	RECOMMENDATIONS TO CURE THE NSA PROGRAM'S ILLEGALITY	462

* Chesterfield Smith Professor of Law and Director, The Center For International Financial Crimes Studies, Levin College of Law, Holland Law Center, University of Florida, Gainesville, FL 32611; Honorary Fellow of Advanced Legal Studies, University of London.

** Research Fellow, The Center For International Financial Crimes Studies, Levin College of Law, Holland Law Center, University of Florida, Gainesville, FL 32611. I would like to thank Professor Fletcher Baldwin for sharing so generously with his time, talents, and scholarship. I would like to thank my brother, William, for his dearly appreciated friendship, my father, Bob for giving me the opportunity to succeed, and my mother, Eileen, who taught me to believe in myself and impressed upon me the value of perseverance. And of course, I would like to thank Jessica, for her love and support, without which, I would never have made it this far.

IV.	CONCLUSION: THE RULE OF LAW: AN ESSENTIAL ELEMENT TO WINNING THE "WAR ON TERROR"	463
V.	EPILOGUE	469

I. INTRODUCTION

The greatest collateral damage from the September 11, 2001, terrorist attacks has been borne by international and domestic law principles in the name of national and homeland security. While it is conceded that one of the primary duties of a constitutional government is to ensure the survival of its governing regime and the physical safety of its citizens, there is an equally important duty for the governing regime to preserve democracy and civil liberties, and to fulfill the duties and obligations assumed under international and humanitarian law. The late U.S. Supreme Court Chief Justice Earl Warren eloquently illustrated this delicate balance of national security interests and democratic principles in his majority opinion in *United States v. Robel*:¹

This concept of "national defense" cannot be deemed an end in itself, justifying any exercise of . . . 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 . . . those liberties . . . which make the defense of the Nation worthwhile.²

Do Chief Justice Warren's words bear directly upon the "war on terrorism"? The hyperbole, as with its predecessor, "war on drugs," wears thin when it reflects a rule by law and no longer communicates a rule of law.

The primary purpose of constitutional law is to maintain domestic and international order so that people may pursue their interests within a predictable legal framework. Such a legal framework depends upon

1. 389 U.S. 258, 264 (1968).

2. *Id.*

judicial interpretation of conflicting assumptions that function and operate within the national psyche.³

As the soul of the constitutional democracy, the rule of law reflects formal and informal obligations and agreements within a constitutional context and includes human rights not subject to majority rule. In this manner, the rule of law facilitates order and respect through expectations. These expectations are essential if society is to survive in a predictable, peaceful and secure fashion.⁴ However, within the context of present circumstances,⁵ Amitai Etzioni⁶ raises several important questions: "Under what conditions is democracy undermined?"⁷ "Are citizens prepared to waive transparency and to give the Chief Executive full power with neither checks or balances?"⁸ Etzioni concluded, "it is a gross misconception to argue that public safety measures entail a sacrifice of rights—or vice versa, that respecting rights entails sacrifices of the common good."⁹

The right to privacy is a traditional American expectation. At present, there is an exceptional tension between non-transparent National Security policies and expectations individuals have regarding civil liberties. Without judicial oversight, such weapons give free reign to one branch of government, the executive. As Justice Scalia suggested in *Kyllo v. United States*,¹⁰ "the sanctity of the home deserves the highest protections of the Constitution."¹¹ Within the sanctity of the home resides an expectation of privacy of the heart, soul and mind. Such expectations run contrary to unsupervised total physical surveillance. Thus, to invade that expectation, government agents must in some manner work within the Fourth Amendment and employ a certain level of judicial scrutiny. Governmental

3. See HOW DID THIS HAPPEN? TERRORISM AND THE NEW WAR (James Hoge & Gideon Rose eds., 2001); ROLAND JACQUARD, IN THE NAME OF OSAMA BIN LADEN : GLOBAL TERRORISM AND THE BIN LADEN BROTHERHOOD (2002). Justice A. Kennedy, in *Roper v. Simmons* 543 U.S. 577, 577 (2005) said: "[T]he United States now stands alone in a world that has turned its face against the juvenile death penalty."

4. See, e.g., LON FULLER, ANATOMY OF LAW (Greenwood Press Reprint, New ed. 1977) (1968); EUGENE WALTER, TERROR AND RESISTANCE (1969); PETER BERGEN, HOLY WAR, INC. (2001). See also Karma Nabulsi, *Just and Unjust War*, in CRIMES OF WAR: WHAT THE PUBLIC SHOULD KNOW 224 (Roy Gutman et al. eds., 1999).

5. Roberta Smith, *America Tried to Come To Terms with Terrorism: The United States Anti-Terrorism and Effective Death Penalty Act of 1996 v. British Anti-Terrorism Law and International Response*, 5 CARDOZO INT'L & COMP. L. 249, 268-69 (1997).

6. AMITAI ETZIONI, HOW PATRIOTIC IS THE PATRIOT ACT? 9 (2004).

7. *Id.* at 9.

8. See generally *id.*

9. *Id.* at 45.

10. *Kyllo v. United States*, 533 U.S. 27 (2001).

11. See *id.* at 31.

privacy invasions have occurred in the past, but none appear as egregious as those reported in the *New York Times* and known as the National Security Agency (NSA) Warrantless Wiretapping Program.¹²

On December 6, 2005, President George W. Bush met in the Oval Office with *New York Times* publisher Arthur Sulzberger, Jr., executive editor Bill Keller, and Washington bureau chief Phil Taubman.¹³ The President called the meeting to discuss the *Times*' plan to publish a story exposing the NSA's covert program that warrantless wiretapping of citizens.¹⁴ The President expressed strong concerns over the national security implications that would result from publishing the article,¹⁵ and implored the *Times* to reconsider.¹⁶ But the free press did not back down.¹⁷

On December 16, 2005, the *New York Times* published a front page story by James Risen and Eric Lichtblau pertaining to the NSA program.¹⁸ The *Times* article focused upon warrantless eavesdropping and suggested that the NSA program was an abuse of executive power.¹⁹ The article, coming almost one year before mid-term elections, ignited a political hailstorm.²⁰ Within days, a judge on the Foreign Intelligence Surveillance Court resigned in protest of the NSA program,²¹ House Democrats investigated the possibility of impeachment,²² and the Senate demanded immediate committee hearings.²³

In response, the Bush Administration reaffirmed the wiretapping program and lashed out against any and all critics.²⁴ The Administration argued that the NSA program was a vital weapon in the war against

12. See Sherman, *infra* note 13.

13. Gabriel Sherman, *Why Times Ran Wiretap Story, Defying Bush*, N.Y. OBSERVER (Dec. 26, 2005), available at <http://observer.com/printpage.asp?iid=12123&ic=Off+the+Record> (last visited July 12, 2006).

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.*

18. Eric Lichtblau & James Risen, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

19. *Id.*

20. See Carol D. Leonnig & Dafna Linzer, *Spy Court Judge Quits in Protest*, WASH. POST, Dec. 20, 2005, at A01.

21. *Id.*

22. Deb Riechmann, *Cheney Says President Has Spying Authority* (Dec. 20, 2005), at <http://breitbart.com/news/2005/12/20/D8EK9JP81.html>.

23. Leonnig & Linzer, *supra* note 20.

24. David Johnston & Neil A. Lewis, *Defending Spy Program, Administration Cites Law*, N.Y. TIMES, Dec. 23, 2005, at A20.

terror.²⁵ Placing the blame on bureaucratic inefficiency, the Administration argued that, in fighting the undeclared “war,” the Constitution must reside in the Oval Office, and the NSA program was the only means permitting the speed and flexibility necessary to give a sufficient warning of an imminent terrorist attack.²⁶

The controversy has yet to be resolved. Defendants and critics have assembled along political fault lines and are prepared to do battle over the program’s constitutionality. Yet, for all the partisan posturing, little about the program is actually known by the public. The Administration’s own statements establish that: (1) the NSA program monitors only international

25. *Id.*

26. *Id.* Did the President’s advisors overlook the Internet? The global reliance of the Internet for commerce, communication, and information, legal and illegal is undisputed. Nonetheless, terrorists, hackers, and organized criminal syndicates also rely on the power and reach of the Internet to serve nefarious ends. For example, it is now widely known that al-Qaeda operatives used (and likely continue to use) Internet chat rooms and free, anonymous e-mail accounts to communicate. Further, captured laptops and debriefs of detained al-Qaeda agents reveal that terrorist interest in the computerized, Internet-connected components of America’s critical infrastructures was both real and serious. Indeed, perhaps future al-Qaeda terrorist attacks will include an assault against the cyber backbone of vulnerable critical infrastructures, such as water supply systems or power generation facilities. Why would terrorists look to the Internet and not the telephone? The answer is surprisingly simple. Attacks in or through cyberspace comport with the terrorists *modus operandi*: asymmetrical warfare. In simple terms, asymmetric warfare is how the weak fight the strong: guerrilla tactics, suicide bombers, ambushes, and nighttime raids. It is also, in our 21st century world, the use of the Internet to exploit, disrupt, or incapacitate disproportionately powerful adversaries. By using cyberspace to conduct intelligence, communicate clandestinely, and even strike remotely, the Internet has now become a new battleground for terrorists like al-Qaeda. With this said, asymmetrical, computer attacks from either al-Qaeda types or teenage hackers do not exist in a vacuum, but are tied to the ubiquitous reliance of the Internet by individuals as well as businesses. The number of Internet users continues to grow, spurred by the falling price of computer technology, the growing accessibility of the Internet in rural areas, the availability of high speed Internet access, and, of course, the overwhelming power and economy of cyberspace. However, security vulnerabilities have become more frequent and more serious. Though not the work of terrorists, 2003 witnessed three major worldwide cyber security: Slammer, SQL, MS Blaster, and Sobig. Collectively, these computer worms cost computer users hundreds of millions of dollars worldwide. Yet, the virulence and effectiveness of Slammer, Blaster, and Sobig can be traced not only to the originality of their programming code but also to the porous security that in 2006 continues to plague computers and the Internet worldwide. The overwhelming majority of personal and business computers still lack firewalls and frequently updated anti-virus software. Government computers continue to suffer break-ins as well. From the sophisticated prospect of cyberterrorism to the lone hacker looking for a cheap thrill, those who use the Internet for illegal ends including sending encrypted terrorist instructions remain undeterred by government “best practices.” There are no conclusive cyber security best practices, yet NSA concentrates upon wiretaps as a “best practice.”

communications between the United States and a foreign country;²⁷ (2) the program is triggered when a non-judicial "career professional" at the NSA has reasonable grounds to believe that one of the parties to a communication is a member of a foreign terrorist organization;²⁸ (3) the program targets U.S. citizens living within the United States;²⁹ and (4) the program does not require a warrant, before beginning surveillance.³⁰

We intend this Article to be a commentary on the constitutionality of the NSA wiretapping program solely as it relates to the warrantless surveillance of U.S. citizens. We will focus upon the legal history as established through case law. We will then attempt to rebut the Administration's arguments in defense of the program, and within this context we will argue that the program cannot withstand legitimate constitutional scrutiny. The facts and law simply do not support the so-called NSA program that authorizes the surveillance.

27. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2006) (statement of Alberto Gonzales, Attorney General of the United States).

28. *Id.*

29. Press Briefing from Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at* <http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html> (last visited July 12, 2006) [hereinafter Press Briefing]. When asked if American citizens were targeted by the NSA program, Attorney General Gonzales responded:

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.

Id.

30. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. On the Judiciary 109th Cong.* (2006) (statement of Alberto Gonzalez, Attorney General of the United States). In lieu of a warrant, the program is triggered when an NSA official has reasonable grounds to believe that one party to the communication is affiliated with al-Qaeda. *Id.* To be absolutely clear, because the program is initiated and supervised by NSA officials, there cannot be a warrant involved since there is no judicial integration in the process.

II. WIRETAPPING—THE GENESIS

A. *Origins*

A recorded directive for warrantless surveillance for national security purposes was detailed in a letter from President Franklin Delano Roosevelt to Attorney General Robert Jackson during World War II.³¹ In that letter, Roosevelt authorized Jackson to secure sensitive information from any person suspected of seditious conduct against the United States.³² President Roosevelt specifically asked Jackson to investigate only non-citizens and exercise considerable restraint.³³

At the time, Roosevelt's directive conformed to the letter of the existing law,³⁴ because the U.S. Supreme Court, in 1928, had concluded that executive wiretapping did not impinge on constitutional rights.³⁵

1. *Olmstead v. United States*³⁶

The issue in *Olmstead* centered around the propriety of governmental use of warrantless electronic surveillance equipment.³⁷ The question was whether the information obtained by electronic surveillance was in violation of the Fourth Amendment and could not be used as evidence in any subsequent prosecution.³⁸ To allow illegally obtained evidence would, in effect, violate the Fifth Amendment's protection against self-incrimination; for if a person's incriminating statement, intercepted illegally, could be used against him in a subsequent prosecution, this would effectively destroy his right to avoid testifying against himself.

In *Olmstead*, federal agents used wiretap devices placed on telephone wires outside the defendant's premises to record incriminating information that led to the subsequent prosecution of the defendant.³⁹ No judicial warrants authorized the wiretaps.⁴⁰

31. Michael Disabatino, *Annotation, Construction and Application of "National Security" Exception to Fourth Amendment Search Warrant Requirement*, 39 A.L.R. FED. 646 (2002).

32. *Id.*

33. *Id.*

34. *Id.*

35. *Olmstead v. United States*, 277 U.S. 438 (1928).

36. *Id.* at 466.

37. *See id.* at 438.

38. *See id.* at 455.

39. *Id.* at 456-57.

40. *See Omstead*, 277 U.S. at 456-58.

The two major issues before the U.S. Supreme Court were: 1) whether such wiretaps constitute an unreasonable search and seizure in violation of the Fourth Amendment; and 2) if so, whether the Fifth Amendment forbids the evidentiary use of such information at trial on the grounds that such evidence would violate the defendant's right not to testify against himself.⁴¹ The Court found that the wiretap did not violate the Fourth Amendment, and therefore, the information obtained could be used in a subsequent prosecution without violating the Fifth Amendment.⁴²

The Court noted that a search warrant would be required before officers could enter the property of a suspect to gather evidence, and that such a warrant would have to be supported by a showing of probable cause that the suspect was engaged in illegal activities. Further, the warrant would have to describe the items sought.⁴³ Although a warrant would be necessary for a search and seizure, the Court found that the Constitution did not protect telephone and telegraph messages:

The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wire beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. We think, therefore, that the wiretapping here disclosed did not amount to search or seizure within the meaning of the Fourth Amendment.⁴⁴

Since there was no physical trespass on the defendant's property, the Court concluded a violation of the Fourth Amendment did not occur.⁴⁵ *Olmstead* thus established the first major criterion by which to judge the legality of warrantless wiretaps.

Justice Brandeis, in dissent, pointed to the dangers of such a restrictive view, noting that: "Time works changes, brings into existence new conditions and purposes. Therefore, a principle to be vital must be capable to wider application than the mischief which gave it birth."⁴⁶ Brandeis also recognized that new electronic innovation created new means of violating

41. *Id.* at 460-62.

42. *Id.* at 466-69.

43. *Id.* at 458-62.

44. *Id.* at 466.

45. *Olmstead*, 277 U.S. at 466.

46. *Id.* at 472.

constitutional protections in ways unforeseen by the Framers of the Constitution.⁴⁷

Citing *Entrick v. Carrington*,⁴⁸ Brandeis argued that it was not the physical trespass that constituted the principal offense to the individual, but the invasion of the individual's privacy that caused the real damage.⁴⁹ Notwithstanding Brandeis's warning, wire and radio communications were deemed subject to warrantless interception.⁵⁰

In 1934, Congress moved to protect radio and wire communications from unauthorized interception by enacting section 605 of the Communications Act.⁵¹ This Act forbade any person from intercepting and divulging interstate wire and radio communications without authorization from the sender of such messages, or without meeting other enumerated conditional requirements.⁵²

2. *Nardone v. United States*⁵³

Since section 605 reads that "no person" may intercept and divulge protected communications to "any person," a question arose as to the applicability of these provisions to federal and state officers, as well as to private individuals. *Nardone v. United States*⁵⁴ was the first opportunity the Supreme Court had to address the confusion surrounding section 605. In *Nardone*, information was uncovered by federal officers through a warrantless wiretap on the defendant's conversations.⁵⁵ The Court held that such evidence was inadmissible in a subsequent prosecution of the defendant. The fact that the eavesdroppers were federal officers did not sway the Court, which said that the statute "is written so as to include within its sweep federal officers as well as others."⁵⁶

Nardone was the Court's attempt to settle the question of the applicability of section 605 to state and federal officers. The case was reheard in 1939.⁵⁷ In the second *Nardone*⁵⁸ case, the Court ruled that even

47. *Id.* at 473.

48. 19 How. St. Tr. 1030 (1765).

49. *Olmstead*, 277 U.S. at 474-79.

50. *See supra* text accompanying notes 37-45.

51. 47 U.S.C. § 605 (1934).

52. *Nardone v. United States*, 302 U.S. 379 (1937).

53. *Id.* at 379.

54. *Id.*; *see also* *Benati v. United States*, 355 U.S. 96 (1957).

55. *Nardone*, 302 U.S. at 379, 381-82.

56. *Id.* at 384.

57. *Id.*

58. *Nardone v. United States*, 308 U.S. 338 (1939).

a paraphrased account of the intercepted communications was inadmissible evidence, when the interception was in violation of section 605.⁵⁹ The Court specified that although a paraphrased account was not a literal divulgence of the precise communications intercepted, nevertheless, such warrantless interception and use was prohibited by the statute and the account was inadmissible as evidence.⁶⁰

The government concluded that at the time President Roosevelt issued the directive, the government, utilizing war powers, could wiretap telephone communications without prior judicial scrutiny.⁶¹ However, President Roosevelt could not legally introduce any of the collected information into trial.⁶² The *Nardone*⁶³ Court concluded that the Federal Communications Act of 1934 prohibited individuals from collecting or distributing information collected via electronic surveillance.⁶⁴ The government conceded that *Nardone* prohibited any information collected in the course of electronic surveillance from being offered into evidence at trial.⁶⁵ There was, however, nothing to prevent police agencies from utilizing wiretaps for national security purposes as long as the information was not "divulged" in a court proceeding.⁶⁶

3. *Katz v. United States*⁶⁷

In *Katz v. United States*,⁶⁸ the post-war U.S. Supreme Court revisited expectations of privacy within the context of wiretapping jurisprudence. Overruling *Olmstead*, the Supreme Court found the use of warrantless electronic surveillance in criminal investigations was per se unreasonable under the Fourth Amendment.⁶⁹ Without a warrant, wiretapping and searches could only be legally conducted pursuant to a "few well-delineated [Fourth Amendment] exceptions."⁷⁰

59. *Id.* at 339-41.

60. *Id.* at 340-41.

61. See Disabatino, *supra* note 31.

62. See Jennifer L. Sullivan, *From "The Purpose" to "A Significant Purpose:" Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment*, 19 NOTRE DAME J.L. 375, 383 (2005).

63. *Nardone*, 302 U.S. at 379.

64. *Id.* at 382.

65. See Sullivan, *supra* note 62, at 384.

66. *Id.*

67. 389 U.S. 347, 357 (1967).

68. *Id.*

69. *Id.* at 375.

70. *Id.*

In *Katz*, the Court rejected the traditional notion that only private property could be protected by the Fourth Amendment and held that “[T]he Fourth Amendment protects people, not places.”⁷¹ In so doing, the Court reversed the defendant’s conviction for transmitting wagering information by telephone in violation of a federal statute.⁷² The FBI had placed a recording device outside the phone booth that recorded the defendant’s end of telephone conversations without first getting a warrant—leading to the defendant’s conviction.⁷³ The U.S. Supreme Court reversed the decision of the lower court, finding that the surveillance failed to meet the preconditions required by the Fourth Amendment.⁷⁴

The U.S. Supreme Court’s reasoning in *Katz*, however, turned on the government’s failure to satisfy the preconditions of the Fourth Amendment in securing a warrant before conducting surveillance, rather than sanctioning the government for conducting clandestine surveillance. The Court has long held that the Fourth Amendment protects individuals against police officers—particularly those officers engaged in the often competitive enterprise of ferreting out a crime—from prematurely making the inferences required to determine probable cause for a search under the Fourth Amendment.⁷⁵ In *Katz*, the Court reversed the defendant’s conviction because the officers did not seek a “neutral and detached magistrate” to make the probable cause determination in accordance with prior case law in *Coolidge v. New Hampshire*.⁷⁶

However, in footnote 23 of *Katz*, the limitations upon the Court become apparent. The Court was divided as to whether the Fourth Amendment contemplated a national security exception.⁷⁷ The majority specifically declined to consider whether such an exception existed.⁷⁸ In his concurrence, Justice White stated that the executive branch did not need a warrant if the President determined that there was a threat to national security.⁷⁹ In a separate concurrence, Justice Douglas stated that the executive branch required a warrant because neither the President nor the Attorney General was capable of acting as a detached and neutral magistrate, as the Fourth Amendment requires.⁸⁰ Therefore, as of the *Katz*

71. *Id.* at 351.

72. *Katz*, 389 U.S. at 359.

73. *Id.* at 349-50.

74. *Id.* at 359.

75. *Johnson v. United States*, 333 U.S. 10, 14 (1948).

76. 403 U.S. 443, 453 (1971).

77. *See Disabatino, supra* note 31.

78. *Id.*

79. *Id.*

80. *Id.*

decision, the U.S. Supreme Court had yet to issue a coherent precedent on warrantless surveillance for national security purposes.

Codifying the *Katz* standard, Congress passed title III of the Omnibus Crime Control and Safe Streets Act (OCCA).⁸¹ Under OCCA, electronic surveillance could only be conducted with a warrant.⁸² Such a warrant could be issued if a judge found probable cause that “an individual is committing, has committed, or is about to commit a particular offense”⁸³ However, like *Katz*, OCCA did not place limits on the President’s discretion to use warrantless wiretaps for national security purposes.⁸⁴ Taking full advantage of the confusion, the executive branch—led by Lyndon B. Johnson and then Richard Nixon—continued warrantless surveillance as if the executive branch possessed complete and unfettered autonomy in national security missions.⁸⁵

B. Keith and the Legality of Wiretapping for Domestic Threats to National Security

In an effort to clarify the legality of warrantless surveillance, the U.S. Supreme Court considered whether the Fourth Amendment contained a national security exception.⁸⁶ In *United States v. U.S. District Court for the Eastern District of Michigan (Keith)*, the government, without prior judicial review, intercepted communications of an individual who conspired to bomb a federal building.⁸⁷ The government argued that warrantless surveillance was necessary to protect the country from “attempts of *domestic organizations* to attack and subvert the existing [government] structure.”⁸⁸ In addition, the government urged that (1) the judicial branch did not have the practical knowledge to determine whether probable cause existed to believe that surveillance was necessary to protect national security and (2) that the inclusion of the judicial branch would result in leaks of sensitive information to the public.⁸⁹ The *Keith* Court agreed that the “covertness and complexity”⁹⁰ of political subversives and

81. See Sullivan, *supra* note 62, at 386.

82. *Id.* (quoting 18 U.S.C. § 3518(3)(a) as amended (2000)).

83. See *id.*

84. See *id.*

85. See *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 311 n.10 (1972).

86. *Id.* at 299.

87. *Id.* at 299-302.

88. *Id.* at 308-09.

89. *Id.* at 319.

90. See *Keith*, 407 U.S. at 311.

their “dependency . . . upon the telephone”⁹¹ makes wiretapping an effective weapon.⁹² However, the *Keith* court was profoundly apprehensive of the invasive nature of electronic surveillance.⁹³ Recognizing that the “broader spirit” of the Fourth Amendment was to shield private communications from unreasonable surveillance,⁹⁴ the *Keith* Court analyzed two central inquiries relating to domestic national security: (1) “whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant”⁹⁵ and (2) “whether a warrant requirement would unduly frustrate the efforts of the government to protect itself.”⁹⁶

In response to the first *Keith* inquiry, the Court held that basic constitutional freedoms are best served through the distinct function of the different branches of government.⁹⁷ According to the Court, judicial review of executive action by a neutral and detached magistrate is the touchstone of preserving privacy and free expression.⁹⁸ As such, the proper function of the branches is for the executive branch to seek a warrant and for the judicial branch to approve the warrant prior to the search.⁹⁹ Specifically citing Justice Douglas’s concurrence in *Katz*, the Court explained that the Fourth Amendment did not contemplate the government as a neutral and detached magistrate because of the government’s responsibility to prosecute and investigate criminal behavior.¹⁰⁰ Thus, the Court held that citizens’ needs for privacy and free expression would be best served by securing a warrant through the judicial branch.¹⁰¹

In response to the second *Keith* question, the Court recognized the validity of the government’s argument that warrantless surveillance was an extremely efficient method of investigation.¹⁰² However, the Court was not convinced that the judicial branch was inept to analyze domestic national security threats.¹⁰³ Rather, the Court responded that the judicial branch was perfectly competent to evaluate whether a warrant was needed

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* at 313.

95. *See Keith*, 407 U.S. at 315.

96. *Id.*

97. *Id.* at 317.

98. *Id.* at 318.

99. *Id.* at 317.

100. *Keith*, 407 U.S. at 317.

101. *See id.* at 320.

102. *See id.* at 319.

103. *Id.* at 320.

because the court regularly dealt with sensitive and complex issues central to domestic national security. Furthermore, the Court found that the involvement of the judicial branch did not create domestic national security vulnerabilities.¹⁰⁴

Concluding the *Keith* analysis, the Court held that domestic government surveillance must comport to the requirements of the Fourth Amendment.¹⁰⁵ Specifically, the Court held that the government must seek the approval of the judicial branch through a warrant prior to the initiation of homeland electronic surveillance.¹⁰⁶ However, the Court expressly reserved judgment on whether the *Keith* analysis applied to the "activities of foreign powers or their agents"¹⁰⁷ outside of the United States.

C. Attempts to Extend the Keith Doctrine to Foreign Threats

The refusal to consider whether the Fourth Amendment contemplated a foreign national security exemption prompted lower courts to fill in the gap.¹⁰⁸ In *United States v. Brown*,¹⁰⁹ the Fifth Circuit Court of Appeals allowed warrantless electronic surveillance for the purpose of protecting national security from a foreign threat.¹¹⁰ Accepting the *Brown* precedent, the Third Circuit, in *United States v. Butenko*,¹¹¹ agreed that the President had the authority to conduct warrantless surveillance against foreign threats to national security.¹¹² However, the *Butenko* court limited the *Brown* decision by stating that the primary purpose of the surveillance must be for foreign security threats, as opposed to the collection of incriminating information for criminal prosecution.¹¹³

Casting the viability of *Brown* and *Butenko* into serious doubt, the U.S. Court of Appeals for the D.C. Circuit strongly questioned the existence of a foreign national security exemption in *Zweibon v. Mitchell*.¹¹⁴ In *Zweibon*, the government used warrantless surveillance against the Jewish Defense League (JDL), an entity composed of American citizens, because the JDL sought to interrupt U.S.-Soviet diplomatic relations through both

104. *Id.* at 320-21.

105. *Keith*, 407 U.S. at 321.

106. *See id.*

107. *Id.* at 321-22.

108. *See Sullivan, supra* note 62, at 388-89.

109. 484 F.2d 418 (5th Cir. 1973).

110. *Id.* at 426.

111. 494 F.2d 593 (3d Cir. 1974).

112. *Id.* at 605.

113. *Id.* at 606.

114. 516 F.2d 594 (D.C. Cir. 1975).

peaceful and violent measures.¹¹⁵ While the *Zweibon* court disfavored any sort of warrantless surveillance, it did not go so far as to deny the existence of a foreign national security exemption.¹¹⁶ Rather, the *Zweibon* court held that the government violated the Fourth Amendment's protections because the JDL was a domestic organization and was not affiliated with any foreign power.¹¹⁷ As such, the *Zweibon* decision put a stop to the rubber-stamping of warrantless surveillance afforded to the executive branch in *Brown* and *Butenko*. This outcome proved to be quite alarming to the Department of Justice as the executive branch previously had few obstacles to conducting electronic surveillance for foreign security purposes.¹¹⁸

At about the same time as the *Zweibon* court heightened judicial scrutiny of warrantless surveillance, the Senate Select Committee to Study Governmental Operations chaired by Senator Frank Church¹¹⁹ (the "Church Committee") voted "to conduct an investigation and study of governmental operations with respect to intelligence activities and of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government."¹²⁰ The Committee's investigation lasted fifteen months and addressed an exhaustive list of issues.¹²¹ The Committee's report contained thousands of pages detailing highly disturbing, questionable, and illegal, activities and programs. These programs targeted U.S. and foreign citizens domestically and abroad, by agencies such as the CIA, FBI, and NSA.¹²²

In response to the question of warrantless surveillance, the Committee reported:

The courts have also not confronted intelligence issues. As the Supreme Court noted in 1972 in commenting on warrantless electronic surveillance, "The practice has been permitted by successive presidents for more than a quarter of a century without

115. *Id.* at 607.

116. *Id.* at 614.

117. *Id.*

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

119. Frank Church Papers, Boise State University, Special Collections Department, Albertsons Library, available at <http://library.boisestate.edu/special/church/church.htm> (last visited Oct. 31, 2006).

120. S. Res. 21, 94th Cong. (1975) (enacted).

121. DONALD J. MUSCH, CIVIL LIBERTIES AND THE FOREIGN INTELLIGENCE SURVEILLANCE 3 (Donald J. Musch ed., 2003).

122. Frank Church Papers, *supra* note 119.

guidance from the Congress or a definitive decision by the Court.”¹²³

The Church Committee then issued as a major finding:

The intelligence community has employed surreptitious collection techniques—mail opening, surreptitious entries, informants, and traditional and highly sophisticated forms of electronic surveillance—to achieve its overly broad intelligence targeting and collection objectives . . .¹²⁴

The Committee added that the legal proceedings and standards regulating the use of such surreptitious collection techniques were insufficient.¹²⁵ In response, the Church Committee recommended additional rules regarding domestic intelligence activities; these recommendations “influenced the passage of the Foreign Intelligence Surveillance Act (“FISA”) of 1978.”¹²⁶

D. The Legislative Response: FISA

The abuses brought to light by the Church Committee included the collection of personal and political information from individuals and organizations including Dr. Martin Luther King, Jr. and the Women’s Liberation Movement.¹²⁷ The Committee’s recommendations and its conclusion that the information collected had no legitimate governmental purpose¹²⁸ resulted in a public outcry for reform.¹²⁹ In fact, the government often collected information simply for the purpose of “stifling domestic dissent [by] giving the incumbent President politically useful information about the opponents . . .”¹³⁰

With the public incensed by the Church Committee Reports and the judiciary eager to abridge executive surveillance power, Congress set out to regulate the executive use of warrantless surveillance.¹³¹ Congress’s efforts culminated in the passage of the FISA, which authorized the executive branch, after securing a warrant, to conduct electronic

123. MUSCH, *supra* note 121, at 3.

124. *Id.* at 4.

125. *See id.*

126. *Id.*

127. Seaman & Gardner, *supra* note 118, at 335.

128. *Id.*

129. *Id.* at 334.

130. *See id.* at 335.

131. *Id.* at 334-36.

surveillance of “foreign powers” and “agents of foreign powers” for “foreign intelligence information.”¹³²

FISA created a specialized court system to grant authorization to conduct electronic surveillance of foreign powers and their agents for foreign intelligence gathering purposes.¹³³ FISA authorizes the Chief Justice of the U.S. Supreme Court to designate seven U.S. district court judges to constitute a lower court (FISA Court), and to designate three judges from U.S. district courts or U.S. courts of appeal to constitute a court of review (FISA Court of Review).¹³⁴ The FISA Court of Review has jurisdiction to review a FISA Court denial of an application submitted under the Act.¹³⁵ If the FISA Court of Review determines that the denial was proper, the U.S. Supreme Court then has jurisdiction to review the decision.¹³⁶

To obtain a warrant under FISA, the executive branch must appeal to the Foreign Intelligence Surveillance Court (FISC), a specially created court of review consisting of federal district court judges.¹³⁷ Under FISA, the FISC will allow surveillance if there is probable cause to believe that the “purpose of the surveillance is to obtain foreign intelligence information.”¹³⁸ In the event of a national emergency,¹³⁹ the President may authorize immediate warrantless surveillance provided that the executive obtains a warrant within seventy-two hours.¹⁴⁰

With a warrant requirement firmly in place, FISA’s approach to surveillance for foreign intelligence has been repeatedly upheld throughout the federal circuits.¹⁴¹ In *United States v. Duggan*,¹⁴² the Second Circuit Court of Appeals held that the warrant mechanism in FISA was “a constitutionally adequate balancing of the individual’s Fourth Amendment rights against the nation’s need to obtain foreign intelligence

132. 50 U.S.C. § 1804(a)(4)(A) (1978).

133. *Id.* § 1803(a).

134. *Id.* § 1803(a), (b).

135. *Id.* § 1803(b).

136. *Id.*

137. *See* 50 U.S.C. § 1803(a).

138. *See id.* § 1804(a)(7)(B). FISA’s probable cause standard was later amended so that law enforcement officials need only demonstrate that “a significant purpose of the investigation” be for foreign security purposes. *See id.* (amended 2001).

139. *See generally In re Sealed Case No. 02-001, 02-002*, 310 F.3d 717 (Foreign Int. Sur. Ct. Rev. 2002) (analyzing this issue).

140. *See* 50 U.S.C. § 1804(f).

141. *See Sullivan, supra* note 62, at 393.

142. 743 F.2d 59 (2d Cir. 1984).

information.”¹⁴³ Likewise, in *United States v. Pelton*,¹⁴⁴ the Fourth Circuit Court of Appeals held that FISA’s reduced probable cause standard was “sufficient protection for the rights guaranteed by the Fourth Amendment”¹⁴⁵ because of the paramount importance of governmental interests in the context of foreign security.¹⁴⁶

With FISA looming in the background, the Fourth Circuit Court of Appeals revisited the familiar issue of executive warrantless surveillance for foreign security threats in *United States v. Truong*.¹⁴⁷ In *Truong*, outside the authority of FISA, and without a warrant, the government wiretapped David Truong, a Vietnamese citizen suspected of passing classified information to the Socialist Republic of Vietnam.¹⁴⁸ Deciding the extent that warrantless surveillance should be allowed for foreign national security, the *Truong* court reexamined the two central inquiries in *Keith* that were relevant to domestic national security threats: (1) whether the needs of citizens would be better protected by requiring a warrant and (2) whether a warrant requirement would unduly frustrate the government’s national security prerogatives.¹⁴⁹

Responding to the first prong of the *Keith* test, the *Truong* court recognized the substantial privacy interests implicated by warrantless surveillance.¹⁵⁰ However, the *Truong* court stated that the intrusion on civil liberties is justified when (1) the surveillance is limited to “foreign powers, their agents, and their collaborators”¹⁵¹ and (2) the surveillance is primarily to “obtain foreign intelligence from foreign powers or their assistants.”¹⁵²

Responding to the second prong, the *Truong* court stated that the warrant requirement would add an unnecessary procedural hurdle that would impede the response to foreign threats.¹⁵³ Further, the *Truong* court reasoned that the executive’s “unparalleled expertise” in foreign affairs made the executive branch the sole entity capable of evaluating the gravity of foreign security threats.¹⁵⁴ Finally, the *Truong* court stated that the

143. *Id.* at 73.

144. 835 F.2d 59 (2d Cir. 1987).

145. *Id.* at 1075.

146. *Id.*

147. 629 F.2d 908, 911 (4th Cir. 1980).

148. *Id.*

149. *Id.* at 913.

150. *Id.* at 916.

151. *Id.*

152. *Truong*, 629 F.2d at 916.

153. *Id.* at 914.

154. *Id.*

Constitution designates the executive as the primary authority in governing international affairs.¹⁵⁵

As a final matter, the *Truong* court recognized that even where a warrant is unnecessary, the Fourth Amendment demands that the surveillance be reasonable in light of the circumstances.¹⁵⁶ The *Truong* court drew the reasonableness line at the point where David Truong became the target of a criminal investigation, and held that warrantless surveillance of foreign security threats was reasonable up to the point where the foreign security threat could be fully evaluated.¹⁵⁷ According to the *Truong* court, the surveillance is no longer reasonable at the point where the individual becomes the subject of a criminal prosecution.¹⁵⁸

E. September 11th and the Genesis of the NSA Program

On September 11, 2001, the al-Qaeda terrorist network launched the most devastating attack ever witnessed on American soil.¹⁵⁹ Decimating critical U.S. economic and military interests, nineteen al-Qaeda terrorists hijacked and crashed four jetliners into the two World Trade Center Towers, the Pentagon, and a field in Pennsylvania.¹⁶⁰ In the span of one hour, the terrorists killed nearly three thousand people, devastated the nation's financial pulse, and awakened America to its own vulnerability.¹⁶¹

Seven days after the September 11th attacks, Congress passed the Authorization for Use of Military Force (AUMF).¹⁶² In the AUMF,

155. *Id.* at 914.

156. *Id.* at 916.

157. *Truong*, 629 F.2d at 916. *Truong* alleged that the search was unreasonable in light of the circumstances because the government intercepted all of his personal communications for over 260 days. *See id.* at 916-17. The *Truong* court held that the search was reasonable up to the point when FBI investigators identified Truong's contact on the other side of the communications. *Id.* at 916 n.6. After that point, Truong became the target of a criminal investigation because the foreign security threat had been fully evaluated. *See id.* at 915-17.

158. *Id.*

159. Letter from the Department of Justice to Members of Congress, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* 1 (Jan. 19, 2006) [hereinafter Department of Justice], available at http://www.globalsecurity.org/intell/library/reports/2006/nsa-authorities_doj060119.htm.

160. *See* Sullivan, *supra* note 62, at 380.

161. *Id.*

162. Authorization for Use of Military Force 50 U.S.C. § 1541 (2001). Section 2 of the AUMF provides, in relevant part, that:

[T]he President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or

Congress granted the President the authorization to “use all necessary and appropriate force”¹⁶³ against those responsible for the September 11th attacks.¹⁶⁴ The government’s response to September 11th was swift and multifaceted.¹⁶⁵ The United States immediately accused the Taliban, the ruling government of Afghanistan, of harboring the al-Qaeda operatives responsible for the September 11th assault.¹⁶⁶ After the Taliban refused to hand over al-Qaeda fugitives, the United States led an offense against the Taliban government beginning on October 7, 2001.¹⁶⁷ Operation Enduring Freedom, the U.S. military response to the September 11th attacks, was swift and ferocious.¹⁶⁸ Ending major combat operations less than a year after the original invasion, the United States began to embark on the arduous task of building a democracy in war-torn Afghanistan.¹⁶⁹

But the global war against terrorism required action in the homeland as well. In an effort to rectify legislative deficiencies in law enforcement and intelligence collection, U.S. lawmakers passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).¹⁷⁰ The Patriot Act lowered the standard of probable cause under FISA so that a law enforcement official could obtain a warrant upon a showing of probable cause that “a significant purpose of the investigation” was for foreign surveillance purposes.¹⁷¹ This lower standard effectively removed the barrier that previously separated criminal investigations from foreign intelligence surveillance under FISA.¹⁷²

harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

50 U.S.C. § 1541(2)(a). Further, section 2 of the AUMF provides, in relevant part, that: “Consistent with [the War Powers Resolution], the Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution.” 50 U.S.C. § 1541(2)(b)(1).

163. *Supra* note 162.

164. *Supra* note 162.

165. *See* Sullivan, *supra* note 62, at 396.

166. Edward Epstein, *U.S. Seizes Skies Over Afghanistan*, S.F. CHRON., Oct. 10, 2001, at A1.

167. *Id.*

168. Bill Nichols, *U.S. Controls Afghan Skies*, USA TODAY, Oct. 10, 2001, at 1A.

169. Larry Copeland, *Afghans Optimistic Assembly Will End Chaos*, USA TODAY, June 10, 2002, at 1A.

170. *See* Sullivan, *supra* note 62, at 380-83.

171. 50 U.S.C. § 1804(a)(7)(B) (amended 2001).

172. *See* Sullivan, *supra* note 62, at 401.

The controversy regarding the NSA program began on December 6, 2005—mere hours after the *New York Times* published its original article on the NSA.¹⁷³ Yet, the NSA wiretapping program had been in existence since President Bush authorized the program in the weeks following the September 11th attacks.¹⁷⁴ The program remains classified, and few critical details have come to light. According to the Bush Administration's statements, the NSA program: (1) intercepts electronic communications;¹⁷⁵ (2) intercepts communications of American citizens inside the United States;¹⁷⁶ (3) operates without the "classical" definition of probable cause;¹⁷⁷ and (4) operates without a warrant.¹⁷⁸ With these facts in mind, the purpose of the following analysis is to evaluate the most pressing question posed by the NSA program: Does the President have the authority to use warrantless surveillance against American citizens living in the homeland?

II. THE PRESIDENT LACKS BOTH THE CONGRESSIONAL AUTHORIZATION AND INHERENT AUTHORITY TO EFFECTUATE THE NSA PROGRAM

On January 19, 2006, the Department of Justice submitted a letter to congressional leaders on behalf of President Bush detailing the Administration's defense of the NSA program.¹⁷⁹ The letter is the fullest, most complete defense the Administration has offered regarding the NSA program. In the letter, the President offers two bases of support for the NSA program: (1) Congress authorized the President to wiretap American citizens without a warrant through the passage of the AUMF; and (2) the

173. See Leonnig & Linzer, *supra* note 20.

174. See President's Radio Address, 41 Weekly Comp. Pres. Doc. 1880 (Dec. 17, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051217.html> (last visited Oct. 19, 2006). In his weekly radio address, the President said: "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-Qaeda and related terrorist organizations." *Id.*

175. Press Briefing, *supra* note 29.

176. *Id.*

177. *Id.* According to Attorney General Gonzales, the NSA program intercepts communications where there is 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." *Id.*

178. *Id.*

179. Department of Justice, *supra* note 159, at 1.

President has the inherent authority as Commander-in-Chief to conduct warrantless surveillance.¹⁸⁰

However, these justifications may not withstand a vigorous constitutional analysis. While President Bush may believe he has the authority for the NSA program, case law in the area of warrantless surveillance does not support the President's argument.¹⁸¹ Congress did not explicitly authorize the President to conduct warrantless surveillance of American citizens by the passage of the AUMF.¹⁸² Furthermore, a careful consideration of the principles articulated in *Keith*, public policy, and in particular its underlying concerns, reveals that the President does not have the inherent authority to conduct warrantless surveillance. Because the President has only questionable congressional or inherent executive authority, the NSA program is unlikely to survive a constitutional challenge.

A. The President Lacks Congressional Authority to Effectuate the NSA Program

President Bush's principal assertion in defense of the NSA program is that Congress unequivocally authorized the executive branch to effectuate the program through the passage of the AUMF.¹⁸³ Relying on *Hamdi v. Rumsfeld*,¹⁸⁴ the President argues that the AUMF provides explicit statutory authority to conduct warrantless surveillance of American citizens who have a link to al-Qaeda.¹⁸⁵ In *Hamdi*, the U.S. Supreme Court considered whether the text of the AUMF enabled the President to capture and detain enemy combatants.¹⁸⁶ Yasser Hamdi, an American citizen allegedly operating as an enemy combatant, was captured and detained after U.S. Forces found him on a battlefield in Afghanistan.¹⁸⁷ Hamdi challenged his detention, arguing that Congress had previously passed a law stating that "[n]o citizen shall be imprisoned or otherwise detained by the United States *except pursuant to an Act of Congress*."¹⁸⁸ As such,

180. *Id.*

181. See *infra* text accompanying notes 241-54.

182. See *supra* text accompanying notes 183-228.

183. Department of Justice, *supra* note 159, at 12.

184. 542 U.S. 507 (2004).

185. See Department of Justice, *supra* note 159.

186. See *Hamdi*, 542 U.S. at 516.

187. *Id.* at 513.

188. See *id.* at 517 (emphasis added) (quoting 18 U.S.C. § 4001(a)).

Hamdi contended that the limited text of the AUMF¹⁸⁹ was an insufficient basis for his detention.¹⁹⁰ Rejecting Hamdi's argument, the Supreme Court interpreted the clause in the AUMF that permitted the President to use "all necessary and appropriate force" to mean that the AUMF authorized the President to engage in all "fundamental incident[s] of waging war. . . ."¹⁹¹ Relying on the Geneva Convention Relative to the Treatment of Prisoners of War and the Hague Convention on Laws and Customs of War on Land, the Court held that the detention of enemy combatants was a fundamental incident of warfare.¹⁹² Accordingly, the text of the AUMF "clearly and unmistakably authorized" the President to detain Hamdi.¹⁹³

President Bush interprets *Hamdi* to mean that the AUMF authorizes the executive branch to conduct all activities that are fundamental incidents of waging war.¹⁹⁴ Citing a robust history of American warfare,¹⁹⁵ the President contends that intelligence collection is a fundamental incident of war.¹⁹⁶ Since the NSA program is a form of intelligence collection, the President insists that the AUMF authorizes him to conduct warrantless surveillance.¹⁹⁷

189. See *supra* text accompanying note 162. According to the Court, the President derived his authority to detain enemy combatants pursuant AUMF language that states the President may use "all necessary and appropriate force" against the "nations, organization, or persons" associated with the September 11th attacks. *Id.*

190. See *Hamdi*, 542 U.S. at 517.

191. *Id.* at 519. Writing for a plurality of the Court, Justice O'Connor stated:

In light of these principles, it is of no moment that the AUMF does not use specific language of detention. Because detention to prevent a combatant's return to the battlefield is a fundamental incident of waging war, in permitting the use of "necessary and appropriate force," Congress has clearly and unmistakably authorized detention in the narrow circumstances considered here.

Id.

192. *Id.* at 519-20.

193. *Id.* at 519.

194. See Department of Justice, *supra* note 159.

195. See *infra* text accompanying notes 202-04.

196. See Department of Justice, *supra* note 159. The Department of Justice Brief states that the interception of communications has been an American war tactic since the Revolutionary War. Specifically, "George Washington received and used to his advantage reports from American intelligence agents on British military strength, British strategic intentions, and British estimates of American strength. One source of Washington's intelligence was intercepted British mail." *Id.* (citations omitted).

197. *Id.*

However, the President may have misplaced his reliance in *Hamdi*. The conduct might only be applicable in the context of a battlefield.¹⁹⁸ In *Hamdi*, Justice O'Connor clarified the scope of the opinion:

[W]e understand Congress' grant of authority for the use of "necessary and appropriate force" to include the authority to detain for the duration of the relevant conflict, and our understanding is based on longstanding law-of-war principles. If the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding may unravel.¹⁹⁹

Thus, while *Hamdi* surely applies to tactics on a battlefield in Afghanistan, the scope of *Hamdi* may not reach endeavors that involve American civilians.²⁰⁰

In evaluating the NSA program, the application of *Hamdi* turns on deciding if the "practical circumstances" of the present war on terror are similar enough to those found in the prior, conventional conflicts that formulated the rules of warfare.²⁰¹ The President argues that intelligence collection is the practical circumstance common to both the present war and conventional warfare. Because intelligence collection has been a vital feature of many wars, the President further asserts that the use of such tactics in the present conflict triggers the application of the *Hamdi* rule.²⁰² Beginning with the Revolutionary War, the President notes that various intelligence collection methods have been used throughout American warfare.²⁰³ For example, George Washington intercepted British mail,²⁰⁴ Civil War generals frequently wiretapped telegraph lines,²⁰⁵ and President Roosevelt authorized warrantless wiretapping against persons suspected of espionage.²⁰⁶ Therefore, the Bush Administration argues that the NSA program falls in line with the *Hamdi* analysis because the larger context

198. Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Congressional Research Service, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information 34 (Jan. 5, 2006) [hereinafter Bazan & Elsea], available at <http://news.findlaw.com/hdocs/docs/nsa/crs10506rpt.pdf> (last visited July 12, 2006).

199. *Hamdi v. Rumsfeld*, 542 U.S. 507, 521 (2004).

200. *Id.*

201. *See id.*

202. *See* Department of Justice, *supra* note 159, at 14-16.

203. *Id.*

204. *Id.* at 15-16.

205. *Id.*

206. *Id.*

of intelligence collection has been used throughout the history of American warfare.²⁰⁷

However, the “practical circumstances” of a war against terrorism are quite unlike those of the “conflicts that informed the development of the law of war.”²⁰⁸ The war against terror is unlike any previous American war. It is a war without borders, without a specific opposing government, without uniforms, and without a clearly discernable enemy acting under color of state. As such, *Hamdi*’s application to the less conventional circumstances of the current conflict, especially those conducted within the United States, may unravel the “understanding” of *Hamdi*.²⁰⁹ Thus, even if the NSA program were found to be a “fundamental incident of war” under *Hamdi*, the program still may be illegal because *Hamdi* likely has no application to tactics waged inside the homeland and far away from the battlefield.

Even if *Hamdi* were found to control the analysis of the NSA program, it is inconclusive whether warrantless surveillance of American citizens meets the AUMF’s requirement that the tactic be a fundamental incident of war.²¹⁰ The *Hamdi* court concluded that the detention of enemy combatants was a fundamental incident of war by referring to the explicit text of both the Geneva Convention and the Hague Convention.²¹¹ However, President Bush has not cited any authority similar in statute that suggests that warrantless surveillance of American citizens is a fundamental incident of war.²¹² Moreover, the President has not cited any international regulation of warfare that suggests that any interception of communications is a fundamental incident of war.²¹³

Additionally, even if *Hamdi* were found to control the constitutional analysis of the NSA program, and warrantless surveillance of American citizens was found to be a fundamental incident of war, the President

207. See Department of Justice, *supra* note 159, at 14-16.

208. See Bazan & Elsea, *supra* note 198, at 33 (citing *Hamdi* (O’Connor, J., concurring)).

209. *Id.*

210. Beth Nolan et al., *On NSA Spying: A Letter to Congress*, 53 N.Y. REV. BOOKS (Feb. 9, 2006), available at <http://www.nybooks.com/articles/18650> (last visited Oct. 19, 2006). As stated by the letter from constitutional scholars: “[i]t is one thing, however, to say that foreign battlefield capture of enemy combatants is an incident of waging war that Congress intended to authorize. It is another matter entirely to treat unchecked warrantless *domestic* spying as included in that authorization . . .” *Id.*

211. *Hamdi v. Rumsfeld*, 542 U.S. 507, 520 (2004).

212. Bazan & Elsea, *supra* note 198, at 35.

213. *Id.* To be fair, there is little doubt that intelligence collection on the battlefield is a fundamental incident of war. But again, the NSA program is a different situation because it involves the surveillance of American citizens on American soil. *Id.*

would still not have congressional authorization.²¹⁴ Congress, through FISA, has already expressly addressed the question of wartime warrantless surveillance, stating that a President may authorize electronic surveillance for up to fifteen days following a declaration of war.²¹⁵ The Supreme Court has consistently held that express and “carefully drawn” statutes supersede general statutes in the event of a conflict.²¹⁶ The President insists that the “necessary and appropriate” clause of the AUMF provides all the necessary authority to conduct unlimited wartime warrantless surveillance—a highly technical, complex, and controversial legal issue. In terms of specificity, the AUMF simply does not compare with FISA.²¹⁷ FISA expressly establishes procedures for domestic wartime surveillance whereas the AUMF broadly grants general authority.²¹⁸ Because FISA specifically establishes procedures for warrantless electronic surveillance, FISA must prevail over the NSA program.

The exclusivity provision contained in section 2511(2)(f) of title III of the OCCA further undermines the President’s arguments.²¹⁹ There, Congress identified FISA²²⁰ as the “exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted.”²²¹ In the Department of

214. See Nolan et al., *supra* note 210, at 3-4.

215. *Id.*

216. See *Int’l Paper Co. v. Ouellette*, 479 U.S. 484, 493-94 (1987). In *Int’l Paper*, the U.S. Supreme Court refused to believe that a statute drawn specifically to address a particular purpose could be thrown into question by a general statutory provision. *Id.*

217. See Nolan et al., *supra* note 210, at 3.

218. *Id.* Under FISA, “[t]he 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.” 50 U.S.C. § 1811.

219. See *supra* text accompanying notes 81-83.

220. See Nolan et al., *supra* note 210, at 3.

221. 18 U.S.C. § 2511(2)(f) (amended 2002). Section (2)(f), reproduced in full, provides:

Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

Justice letter, the President claims that the OCCA exclusivity provision supports the legality of the NSA program:

By expressly and broadly excepting from its prohibition electronic surveillance undertaken “as authorized by statute,” section 109 of FISA [18 U.S.C. 1809] permits an exception to the “procedures” of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).²²²

According to President Bush, OCCA declares FISA to be the exclusive protocol for electronic surveillance, and FISA, in return, allows another statute—in this case the AUMF—to authorize electronic surveillance. To be specific, the President refers to section 109 of FISA because it prohibits all electronic surveillance conducted “under color of law except as authorized by statute.”²²³ Under the President’s conception, the AUMF provides the necessary statutory exception required by that provision. Therefore, in the President’s view, the OCCA exclusivity provision does not bar the NSA program because FISA actually authorizes electronic surveillance via the AUMF.²²⁴ But if this were correct, the exclusivity provision would essentially be rendered meaningless because it would not exclude anything.²²⁵ If the President were correct, then the text of the OCCA section should read to prohibit electronic surveillance except “as authorized by FISA or *any other statute*.”²²⁶ To accept the President’s argument, one must believe that Congress, by passing a statute that declared FISA the exclusive protocol for electronic surveillance, actually intended that FISA be exclusive—but so is any other statute that

Id. While the aforementioned statute is long and complex, a careful reading clearly demonstrates that FISA is the exclusive authority for “electronic surveillance.” *Id.* To restate, while foreign intelligence may be collected by other specifically mentioned statutes, only FISA is the authority on electronic surveillance. Also, please note that section “101” of FISA became § 1801.

222. Department of Justice, *supra* note 159, at 23.

223. 50 U.S.C. § 1809(a)(1). Section 1809(a)(1) provides, in relevant part, that a “person is guilty of an offense if he intentionally engages in electronic surveillance under color of law except as authorized statute.”

224. William Moschella, Asst. Attorney General, Department of Justice, Letter to Chairman of the Senate Select Committee on Intelligence (Dec. 22, 2005) [hereinafter Letter from Moschella], at <http://www.epic.org/privacy/terrorism/fisa/nsaletter122205.pdf>.

225. Bazan & Elsea, *supra* note 198, at 41.

226. *See id.* at 40. Bazan and Elsea focus on section 2511(2)(e) when stating that the provision should be read to exempt electronic surveillance “as authorized by FISA or *any other statute*.” However, since the President takes the same approach to OCCA’s exclusivity provision, Bazan and Elsea’s analysis is equally applicable. *Id.*

implicates electronic surveillance. On that basis, it is a fair inference that the true intent of Congress in passing an *exclusivity* provision was to actually make FISA's comprehensive statutory scheme the *exclusive* means to conduct electronic surveillance.

Moreover, Congress last reviewed the OCCA exclusivity provision on November 25, 2002,²²⁷ which was two months after the passage of the AUMF. According to the Bush Administration, congressional leaders were briefed on the NSA program "more than a dozen times."²²⁸ The President's argument implies that Congress gave its silent acquiescence to the program by not changing the parameters of section 2511(f) upon receiving knowledge as to the mechanics of the NSA program. However, the President cannot plausibly suggest that Congress's inactions were an official approval of the NSA program. In fact, it is *because* Congress was aware of the NSA program, yet chose not to affirmatively sanction the program, that the legality of the NSA is now in doubt.

The reasons for this doubt are: (1) the President's reliance on the *Hamdi* precedent may be misplaced; (2) the President has failed to demonstrate that the warrantless surveillance of American citizens is a "fundamental incident of war"; and (3) Congress most likely intended that FISA's comprehensive regulations be the exclusive protocol for warrantless surveillance, the President appears to lack congressional authorization to effectuate the NSA program.

B. *The President Lacks the Inherent Authority to Effectuate the NSA Program*

In the seminal opinion of *Youngstown Sheet & Tube Co. v. Sawyer*,²²⁹ Justice Jackson discussed the latitude of discretion afforded to a President whose acts defy the will of Congress:

When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his constitutional powers minus any constitutional powers of Congress over the matter. 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

227. See 18 U.S.C. § 2511 (2002).

228. Letter from Moschella, *supra* note 224, at 1.

229. 343 U.S. 579 (1952).

scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.²³⁰

Because the NSA program is at odds with FISA, the President's power is at its lowest ebb. Therefore, the legality of the program is cast into serious doubt. Thus, the President must rely on his inherent executive authority under Article II of the Constitution in order to effectuate the NSA program.

Relying on his role as Commander-in-Chief and his authority as the final arbiter of international relations, the President asserts that the Constitution compels him to "protect the Nation from foreign attack."²³¹ The President argues that he must have the "authority to gather information necessary for the execution of his office."²³² Additionally, the President insists that he enjoys a heightened level of authority because he is presently acting as the Commander-in-Chief during wartime.²³³

While the President is correct that he enjoys substantial authority in international relations²³⁴ and in his capacity as Commander-in-Chief,²³⁵ the President's actions must still comport to the rest of the Constitution.²³⁶ As a separate consideration in *Hamdi*, the Supreme Court held that a President, even while acting in the course of his capacity of Commander-in-Chief, must do so under the precepts of the Constitution.²³⁷ To that end, even if the President has the inherent authority to conduct warrantless surveillance of some sort, his activities must comport to Fourth Amendment standards.²³⁸

230. *Id.* at 637-38. (Jackson, J., concurring).

231. *See* Department of Justice, *supra* note 159, at 4.

232. *Id.*

233. *Id.*

234. *See* *United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304, 319 (1936). The U.S. Supreme Court has stated "[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." *Id.*

235. *See* *Chi. & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948).

236. *See* *Hamdi v. Rumsfeld*, 542 U.S. 507, 532-35 (2004).

237. In *Hamdi*, the U.S. Supreme Court concluded that, even though the President had the authority to detain Yasser Hamdi as an enemy combatant, Hamdi must still be afforded his due process rights. *See Hamdi*, 542 U.S. at 533-36. By analogy then, the President must observe the requirements of the Fourth Amendment in the course of his duties as Commander-in-Chief.

238. The Fourth Amendment of the Constitution, reproduced in full, provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and

The U.S. Supreme Court has expressly declined to consider whether the Fourth Amendment allows the executive branch to conduct warrantless surveillance against American citizens for security from foreign threats.²³⁹ Despite the lack of precedent, the *Keith* case offers the most direct and relevant mode of analysis in the evaluation of the NSA program.²⁴⁰ The legality of the NSA program turns on the two central *Keith* inquiries: (1) “whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant”²⁴¹ and (2) “whether a warrant requirement would unduly frustrate the efforts of Government to protect itself.”²⁴²

In response to the *Keith* analysis, the President insists that he has the inherent authority to conduct the NSA program because the “President has uniquely strong constitutional powers in matters pertaining to foreign affairs and national security.”²⁴³ It is true that President Bush enjoys a heightened authority as Commander-in-Chief in the realm of foreign affairs. But, as stated by Justice O’Connor, this heightened authority “is not a blank check for the President when it comes to the rights of the Nation’s citizens.”²⁴⁴

Examining the NSA program under the first tier of the *Keith* analysis, the citizens’ needs for privacy and free expression would unquestionably be best protected by requiring a warrant. The *Keith* court recognized that the commands of the Fourth Amendment cannot be swept aside for the sake of administrative efficiency.²⁴⁵ On behalf of the *Keith* majority, Justice Powell wrote:

The warrant clause of the Fourth Amendment . . . has been a “valued part of our constitutional law for decades, and it has

particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

239. See *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 321-22 (1972).

240. In support of his assertion that the NSA program comports to the standards of the Fourth Amendment, the President cites: *United States v. Truong*, 629 F.2d 908, 913-14 (1980); *United States v. Butenko*, 494 F.2d 593, (3d Cir. 1974); and *United States v. Brown*, 484 F.2d 418, 425-26 (5th Cir. 1973). See Department of Justice, *supra* note 159, at 5. These cases all implicate *Keith* as the starting point for the analysis of the President’s authority to conduct warrantless surveillance.

241. See *Keith*, 407 U.S. at 315.

242. *Id.*

243. See Department of Justice, *supra* note 159, at 5.

244. *Hamdi v. Rumsfeld*, 542 U.S. 507, 537 (2004).

245. See *Keith*, 407 U.S. at 315.

determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be 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 party of any system of law enforcement."²⁴⁶

There is no substitute for a warrant based on probable cause to protect the rights of citizens. The warrant requirement ensures that the public will be free from undue and burdensome governmental intrusion. Yet in contravention of this essential constitutional command, the NSA program does not require a warrant.²⁴⁷ The absence of this crucial constitutional protection undermines the legality of the program.²⁴⁸

Instead of a warrant, the NSA program operates on a standard of suspicion that has never been recognized by the U.S. Supreme Court, or any other court. The NSA program is triggered when the Administration has 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."²⁴⁹ The NSA program's impossibly broad standard is nearly infinite in application.²⁵⁰ As suggested by Professor Laurence Tribe,²⁵¹ "a United States citizen living here who received a phone call from another United States citizen who attends a mosque that the administration believes is 'supportive' of al-Qaeda could be wiretapped without a warrant."²⁵² The lack of a workable standard of probable cause forces the conclusion that the privacy rights of citizens would best be protected by requiring a warrant.

Worst of all, the NSA program is an unchecked exercise of executive power. In the NSA program, only the executive branch concludes whether an individual is affiliated with al-Qaeda.²⁵³ In *Keith*, Justice Powell recognized the inherent danger of that situation:

246. See *id.* (quoting *Coolidge v. New Hampshire*, 408 U.S. 443, 481 (1971)).

247. Press Briefing, *supra* note 29, at 2.

248. See Nolan et al., *supra* note 210, at 6.

249. Press Briefing, *supra* note 29, at 1.

250. See Nolan et al., *supra* note 210, at 6.

251. Laurence Tribe is a constitutional law scholar and the Carl M. Loeb Professor of Law at Harvard University, at www.law.harvard.edu/faculty/directory/facdir.php?id=74 (last visited Oct. 19, 2006).

252. *Id.*

253. Press Briefing, *supra* note 29, at 2.

Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate and to prosecute. 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 speech.²⁵⁴

The NSA program is plagued with a conflict of interest. It is devoid of judicial intervention. Without the cooperation of the judiciary, there is no check on law enforcement officials who are quick to ignore potential errors in judgment when the prosecution of a suspected terrorist is in sight. It is irrelevant that the Administration has the best intentions of ending global terrorism; the NSA program is simply too susceptible to abuse. The failure of the Administration to integrate the judicial branch undermines the indispensable system of checks and balances on which this government is based. As such, the program raises significant concerns under the Fourth Amendment.

As necessary as a warrant may be, the President may still be able to continue the NSA program if he can prove under the second tier of *Keith* that obtaining a warrant would unduly frustrate the intent of the government to protect the nation from foreign security threats. President Bush relies primarily on the reasoning articulated in *Truong*²⁵⁵ to demonstrate that a warrant requirement poses an undue burden under the *Keith* analysis.²⁵⁶ As stated in Part I, *Truong* held that a warrant requirement may be unnecessary for foreign security because: (1) a

254. *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 316-17 (1972).

255. To be fair, the President also relies on *Brown* and *Butenko* to assert that he has the inherent authority to conduct warrantless surveillance. He states:

[t]he courts uniformly have approved this longstanding Executive Branch practice. Indeed, every federal appellate court to rule on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant.

Department of Justice, *supra* note 159, at 5. This Article will respond to the *Truong* analysis because it is the clearest and most recent opinion and *Truong* was decided in the wake of FISA.

256. *Id.* at 9.

warrant requirement places an inefficient procedural hurdle on the President;²⁵⁷ (2) the executive branch is an expert on foreign affairs;²⁵⁸ and (3) the Constitution designates the President as the authority in international affairs.²⁵⁹ As such, the President contends he has inherent authority to authorize warrantless surveillance for the reasons set forth in *Truong*.²⁶⁰

The President's arguments are not unique. The cited reasons for excusal from the warrant requirement were considered and rejected by the *Zweibon* court.²⁶¹ While still mindful of the President's substantial grant of power in the realm of foreign affairs, the *Zweibon* court—over thirty years ago—confronted the arguments that the President advances today.²⁶² The *Zweibon* court found that the warrant requirement was not an inefficient procedural hurdle because judges are not “insensitive or uncomprehending of the issues involved in foreign security,”²⁶³ and therefore the judges “will not deny any legitimate requests for a warrant.”²⁶⁴ The *Zweibon* court recognized that the executive branch was the expert on foreign affairs.²⁶⁵ However, the Court noted that the judicial branch was perfectly capable of understanding the complexities and dimensions of the international arena.²⁶⁶ As stated in *Zweibon*, “If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.”²⁶⁷ Finally, while the Constitution does designate the President as the authority in international affairs, the *Zweibon* court reasoned that the President's authority must be tempered with careful judicial scrutiny.²⁶⁸ In short, a warrant requirement does not pose an undue burden on the executive branch.

257. *United States v. Truong*, 629 F.2d 908, 913 (4th Cir. 1980).

258. *Id.* at 914.

259. *Id.*

260. *See* Department of Justice, *supra* note 159, at 5.

261. *See supra* text accompanying notes 262-67.

262. *See Zweibon v. Mitchell*, 516 F.2d 594, 640-44 (D.C. Cir. 1975).

263. *Id.* at 641-42.

264. *Id.* at 642.

265. *See id.* at 641 n.120.

266. *Id.* at 641.

267. *Zweibon*, 516 F.2d at 641.

268. *Id.*

III. RECOMMENDATIONS TO CURE THE NSA PROGRAM'S ILLEGALITY

As a matter of policy, it is important to recognize the undeniably grave concerns faced by the executive branch in a time of war. The President argues:

[T]he Government's interest in engaging in the NSA activities is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack already has taken thousands of lives and placed the Nation from attack is perhaps the most important function of the federal Government—and one of the few express obligations of the federal Government enshrined in this Constitution.²⁶⁹

The President is correct in his assessment of the gravity of the threat of global terrorism. To that end, he must have all the appropriate tools to counter that threat. But the President has a lawful and effective weapon at his disposal in FISA. FISA strikes the appropriate balance between the necessity of law enforcement and the protection of civil liberties. On the other hand, the NSA program is a threat to all the rights of every citizen for privacy and free expression. Thus, the NSA program should be revised in a manner that would make it consistent with FISA and the Constitution.

First, to cure any question of illegality, the President should command the administrators of the NSA program secure a warrant prior to surveillance of an individual. The Supreme Court has long recognized that a warrant, based on probable cause, adequately protects an individual's right to privacy.²⁷⁰ A warrant requirement would integrate the judicial branch into the NSA program. The courts, a neutral and detached third party, would be able to evaluate the evidence against an individual and determine whether the intrusion is justifiable. After a court has granted a warrant, the executive branch is free to pursue an aggressive surveillance of the individual suspected of terrorist behavior.

The current level of suspicion required to effectuate the NSA program must be elevated so that it resembles a standard of probable cause already sanctioned by the courts. The Patriot Act amended FISA so that the executive may secure a warrant for electronic surveillance based on probable cause that a "significant purpose of the investigation" is for foreign intelligence purposes.²⁷¹ The Foreign Intelligence Surveillance

269. See Department of Justice, *supra* note 159, at 20.

270. See *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 315-17 (1972).

271. 50 U.S.C. § 1804(a)(7)(B) (amended 2001).

Court of Review, the appellate branch of FISA, determined that this reduced standard of probable cause has been recognized as an adequate safeguard of civil liberties.²⁷² The current standard of the NSA program, that one is “affiliated” with al-Qaeda, should be elevated so that the NSA program is in line with standing precedent of a legally recognized standard of probable cause.

In the event that securing a warrant is impossible because of the imminence of an attack, the NSA program should conform to the provisions of FISA. Under § 1805(f) of FISA, the President may authorize instant electronic surveillance of an individual provided that the executive branch received a warrant within 72 hours.²⁷³ If the NSA program conformed to § 1805(f), the President would be adequately able to respond to emerging terrorist threats while still providing due deference to civil liberties.

Amending the NSA program will provide the President with an effective means to defend the nation from a terrorist attack and win the war against terror. By requiring a warrant, elevating the standard of probable cause, and providing an emergency surveillance provision, the NSA program will also protect civil liberties. With these recommendations in effect, the NSA program could be a valid and effective tool against terror that is fully consistent with the Constitution.

IV. CONCLUSION: THE RULE OF LAW: AN ESSENTIAL ELEMENT TO WINNING THE “WAR ON TERROR”

It is lamentable, that to be a good patriot one must become the
enemy of the rest of mankind. —Voltaire

America will never be destroyed from the outside. If we falter,
and lose our freedoms, it will be because we destroyed ourselves.
—Abraham Lincoln

These final thoughts are an expansion of earlier efforts to find the
elusive middle ground between a rule of law and a rule by law post 9/11.²⁷⁴

272. *In re Sealed Case No. 02-001*, 310 F.3d 717, 719-20 (Foreign Int. Sur. Ct. Rev. 2002).

273. 50 U.S.C. § 1805(f) (2006).

274. *Supra* text accompanying note 2.

There are currently two ongoing debates regarding the rule of law within the context of the war on terror. On the one hand, we have those who argue that the war on terror is a “new paradigm” that does not neatly lend itself to the rules and norms of international law or to traditional U.S. democratic principles such as the right to due process, the right of privacy, the freedom of association.²⁷⁵ This position is summed up by U.S. Vice President Cheney who exclaimed that the United States “must be—willing to go to the ‘dark side’ to fight terrorism” and that “[a] lot of what needs to be done here will have to be done quietly, without any discussion.”²⁷⁶

The war on terror is summarily and singularly about overwhelming, supreme emergencies where there is no time for debate, deliberation, or choice. The “war” necessitates unprecedented governmental opacity, secrecy, intrusion, and renders “quaint”²⁷⁷ the traditional rules of war and democratic values of due process, equal protection, privacy, and human dignity enshrined within the U.S. Constitution and international agreements.²⁷⁸ Reducing the war on terror to exigent circumstances is sheer fantasy—constituent consumption, intended to be consumed without pause of thought. Attempts at limiting the entire debate on how best to

275. Robert O. Boorstin, *Memorandum on the Geneva Conventions: Tossing Aside the Geneva Conventions, Bush Decisions Place U.S. Troops in Greater Danger*, May 18, 2004, at <http://www.americanprogress.org/issues/kfiles/b79532.html> (last visited Oct. 19, 2006); U.S. Attorney General Alberto Gonzales, *Memorandum for the President of the United States, Decision Regarding Application of the Geneva Conventions of War to the Conflict with al-Qaeda and the Taliban*, January 25, 2002, available at <http://www.msnbc.msn.com/id/4999148/site/newsweek/> (last visited Oct. 19, 2006). See generally DAVID COLE & JAMES X. DEMPSEY, *TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY* (2002); see also DAVID COLE, *ENEMY ALIENS: DOUBLE STANDARDS AND CONSTITUTIONAL FREEDOMS IN THE WAR ON TERRORISM* (2003).

276. Elisa Massimino, *Heading Toward the ‘Dark Side,’* L.A. TIMES, Nov. 21, 2005, at B11, available at <http://www.commondreams.org/views05/1121-25.htm> (last visited Oct. 19, 2006); The Vice President Appears on Meet the Press with Tim Russert, Sept. 16, 2001, available at <http://www.whitehouse.gov/vicepresident/news-speeches/speeches/vp20010916.html> (last visited July 12, 2006).

277. Gonzales, *supra* note 275.

278. See, e.g., David E. Sanger & Eric Schmitt, *Bush Says He’s Confident That He and McCain Will Reach Agreement On Interrogation*, N.Y. TIMES, Dec. 13, 2005, at A22, available at <http://www.nytimes.com/2005/12/13/politics/13detain.html> (July 12, 2006) (describing how the White House “prefers, in background conversations, to talk about the ‘doomsday scenario’: What would happen if the president believed a nuclear device had been planted in an American city, and interrogators had just minutes to extract information about its location from a terror suspect?” and quoting William H. Taft, IV, who served as the State Department’s legal advisor during President Bush’s first term, that Senator John McCain’s amendment to ban inhumane and degrading treatment of detainees “calls for conduct to be consistent with the Army field manual, but doesn’t presuppose what that is to be”).

combat global terrorism to a false premise based upon ticking time bombs and imminent attacks from terrorists and rogue states is a political ploy that has little to do with reality in most cases. Will the result of such interference be civil war?

In reality, the lion's share of combating global terrorism comprises a web of complexities. Its components include methodically and painstakingly acquiring bits of intelligence and piecing them together into a larger mosaic. By seizing and freezing assets of terrorists and terrorist organizations, implementing foreign policies and employing diplomatic pressure on states susceptible to terrorist activities, a responsible war on global terrorism can be waged. Many terrorist plots, including the 9/11 attacks on the United States, are not planned or carried out in minutes, hours, or even days. They appear to be the product of patient and methodical planning by terrorists over the course of years and span several continents.²⁷⁹

In all but the most extreme circumstances, combating global terrorism should be a deliberate, debatable, multilateral undertaking; the combat efforts should always operate within the parameters of the rule of law. The Framers of the U.S. Constitution appeared to concede that the office of the chief executive needed to exercise a limited amount of secrecy,²⁸⁰ speed,

279. See Maria Ressa, *Ressa: Hambali the al Qaeda, Jemaah Islamiyah Link*, CNN.COM, Aug. 14, 2003, available at <http://www.cnn.com/2003/WORLD/asiapcf/southeast/08/14/otsc.ressa/index.html> (last visited July 12, 2006). Riduan Isamuddin, a key al-Qaeda figure in Asia who is also known as Hambali and one of the leaders of Jemaah Islamiyah, al-Qaeda's arm in Southeast Asia,

organized a meeting of about half a dozen al-Qaeda senior leaders in Malaysia in 2000, which basically was one of the first planning sessions of the 9/11 attack. Among the leaders who attended those meetings was the man who was believed to be the mastermind of the "USS Cole" as well as the bombing operations within Southeast Asia, itself. Three of the September 11 hijackers were also at that meeting.

Id.; see also CNN presents: *Seeds of Terror*, CNN television broadcast, aired June 15, 2003, (tracing the roots of al-Qaeda to Southeast Asia, based on a terrorist plot that occurred in that region in 1995, which was a blueprint for what happened on September 11, 2001). See also JEAN-CHARLES BRISARD & GUILLAUME DASQUIE, *FORBIDDEN TRUTH: U.S.-TALIBAN SECRET OIL DIPLOMACY AND THE FAILED HUNT FOR BIN LADEN* (2002).

280. THE FEDERALIST No. 64, at 394 (John Jay) (recognizing the need for "perfect SECRECY and immediate DESPATCH [sic]" within the executive in order for him or her to execute treaties and for "the business of intelligence," when "the most useful intelligence may be obtained, if the persons possessing it can be relieved from apprehensions of discovery"); but see Bill of Rights, U.S. CONST. amend. I, III, IV, V VI, IX, & XIV.

and dispatch to protect the national security of the United States.²⁸¹ The Framers, having an aversion to unaccountable standing armies, also agreed that significant war powers would be vested in Article I, the legislative branch, as a means of establishing a check on the executive's powers as Commander-in-Chief.²⁸² The Framers' fear of limitless power of the executive *vis-à-vis* as Commander-in-Chief of the armed forces is evidenced in the Declaration of Independence and in the Bill of Rights—the latter serving as a further check on executive power. Thus, while it is fairly clear that the President has some powers under Article II to preserve, protect, and defend the nation as Commander-in-Chief, it is also equally clear that those powers were never intended to be plenary.²⁸³ If this were so, then we would have no need for little inconveniences such

281. See U.S. CONST. art. II, § 2 ("The President shall be the Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States . . ."); see also *id.* art. II, § 1 (stating the President has a fundamental duty to "preserve, protect, and defend the Constitution"); *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297 (1972). Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President—through the Attorney General—may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government. *Id.* at 310; but see U.S. CONST. art. III; *Keith*, 407 U.S. at 316.

Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch . . . [t]he 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.

Keith, 407 U.S. at 316.

282. U.S. CONST. art. I, § 8 ("Congress shall have power To . . . provide for the common Defence . . . To declare War . . . To raise and support Armies . . . To provide and maintain a Navy . . . [and t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution . . .").

283. See, e.g., *United States v. Ehrlichman*, 376 F. Supp. 29, *aff'd*, 546 F.2d 910 (D.C. Cir. 1976), *cert. denied*, 429 U.S. 1120 (1977) (explicating at note 4 "The doctrine of the President's inherent authority as 'the sole organ of the nation in its external relations,'" 10 ANNALS OF CONG. 613 (1800) (remarks of John Marshall); *United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304, 319 (1936). None of these cases purport to deal with the constitutional rights of American citizens or with presidential action in defiance of congressional legislation. When such issues have arisen, executive assertions of inherent authority have been soundly rejected. See *Kent v. Dulles*, 357 U.S. 116, 129-30 (1958); *Youngstown Sheet & Tubing Co. v. Sawyer*, 343 U.S. 579 (1953); see also U.S. CONST. art. II, § 3 (establishing that the President of the United States "shall take Care that the Laws be faithfully executed . . ."); *id.* art. II, § 1 (affirming that the President shall "preserve, protect and defend the Constitution of the United States").

as having Congress battle over whether or not certain provisions of the Patriot Act should be extended, made permanent, or scrapped entirely. President Bush, acting under Article II, could simply authorize the Patriot Act's mandates without congressional or judicial participation, and a police state would be created. Thus, we would have the President functioning under the rule by law and no longer under the constitutional rule of law.²⁸⁴

While it is conceded that one of the primary duties of any government is to ensure the survival of its legitimate governing regime and the physical safety of its citizens, an equally important duty is to preserve democracy and civil liberties and to fulfill obligations mandated under national, international, and humanitarian law.

Are Chief Justice Warren's words applicable to the "war on terrorism"?²⁸⁵ The answer is problematic, because the judicial branch of the U.S. government has just begun to awake from its post 9/11 slumber and is considering constitutional values within the context of the present crisis. The Supreme Court, long before 9/11, introduced a crime control model of governance which is now firmly in place.²⁸⁶ The President and attorney general continually speak in terms of a "war on terror," however, this is a war that is both undeclared and unending. Since *Marbury v. Madison*,²⁸⁷ judicial review has been constitutionally mandated where constitutional issues emerge.²⁸⁸

No one objects to a society seeking to protect itself and its institutions from assault, regardless of whether the threat comes from at home or abroad. However, within a constitutional democracy model, protection includes democratic values that are enshrined within one's constitution. It is unacceptable to infringe upon and subvert human rights unless a tested, factual basis for infringement emerges.²⁸⁹ This is supposed to be the goal of judicial review. It is not appropriate for a President to create law through speeches to selected receptive audiences or a cowering press. Governmental intervention must be constitutionally tested within the

284. See Fletcher Baldwin, *The United States Supreme Court: A Creative Check of Institutional Misdirection*, 45 IND. L.J. 550 (1970); see also Zagaris, *infra* note 290.

285. See *supra* text accompanying note 2.

286. Aharon Barak [President of the Supreme Court of Israel], *A Judge on Judging the Role of a Supreme Court in a Democracy*, 116 HARV. L. REV. 19, 27-46 (2002).

287. 5 U.S. 137 (1803).

288. See Barak, *supra* note 286, at 121-22.

289. See generally H.L.A. HART, *THE CONCEPT OF LAW* (1961).

context of compelling credentials.²⁹⁰ None have been shown in the present case.

Anthony Lewis, *New York Times* editorial writer and author of the book *Gideon's Trumpet*, articulated this more succinctly in the inaugural of the Joseph M. Reck, Distinguished Lecture Series at Emory University on March 19, 2003. Anthony Lewis's conclusion merits repeating. Summarizing the nature of the present administration's policy towards enemy combatants he stated:

This is the crux of the *Padilla* case. Jose Padilla is not a person with a sympathetic record. But what matters is not his person, but the breadth of the claim made by Ashcroft and his lawyers. It is that they can keep any American citizen—any of us—in prison for the rest of our lives, in solitary confinement on the say so of government officials, with no check except the rather slim possibility of a judge finding that the government did not have any evidence.

The administration argues that requiring it to treat Padilla with constitutional fairness would “significantly hamper the nation's defense.” But if there is anything about which the press should be skeptical, it is such assertions that the national security would be at risk if courts applied the Constitution. For those claims have turned out to be wrong again and again.

The Pentagon Papers case was an outstanding example. If the *New York Times* were allowed to publish its series on the origins of the Vietnam War, the government said, national security would be gravely damaged. On the fourth day of publication of the *Times'* lawyer, [the late Professor] Alexander Bickel, observed drily to the judge:

“Your Honor, the republic still stands.”²⁹¹

290. See Bruce Zagaris, *U.S. District Court Reiterates U.S. Terror Suspect's Right to Counsel*, 19 INT'L ENFORCEMENT L. REP. 183 (2003).

291. Fletcher N. Baldwin, Jr. & Theresa A. DiPerna, *The Rule of Law: An Essential Component of the Financial War Against Organized Crime and Terrorism in the Americas* (unpublished conference materials), available at www.law.ufl.edu/cgr/conference/06confmaterials/2_Panel/2_FletcherBaldwin-Dipernaterrorism.pdf; Anthony Lewis, *Wake Up America*, N.Y. TIMES, Nov. 30, 2001, at A27, available at <http://www.commondreams.org/views01/1130-05.htm> (last viewed July 12, 2006). See Fletcher Baldwin, *The Rule of Law*,

V. EPILOGUE

There should be no objection to a government protecting its people from assaults originating at home or from abroad. Protection, however, is only one factor in an array of constitutional principles. It is unacceptable to implement secret programs that diminish constitutional values while engaged in doublespeak policies. To defer to constitutional values and to diminish them, requires, at the least, a tested factual basis—not a sparse conclusion of efficacy. Herein lies the goal of Article III of the U.S. Constitution.

On January 17, 2006, the American Civil Liberties Union, together with a collection of journalists, academics, and attorneys who maintained regular communication with persons who allegedly had links to al-Qaeda, filed a complaint against the NSA challenging the constitutionality of the warrantless wiretapping program.²⁹²

On August 17, 2006, U.S. District Court Judge Taylor issued an opinion in the case of *American Civil Liberties Union v. National Security Agency*.²⁹³ In that opinion, Judge Taylor concluded that the wiretapping program was an unconstitutional exercise of executive power.²⁹⁴ The secret wiretapping impermissibly burdened the First and Fourth Amendment rights of the plaintiffs.²⁹⁵ The plaintiffs asserted that the government violated their Fourth Amendment rights in several ways such as: 1) seizing their constitutionally protected communications without a warrant;²⁹⁶ 2) the program also violated First Amendment rights by the chilling effect of constant random surveillance;²⁹⁷ and 3) the program exceeded the constitutional grant of executive power under the Separation of Powers doctrine.²⁹⁸

The court noted that the wiretaps were a seizure that triggered the Fourth Amendment's protection against yielding "too readily to pressures

Human Rights and Proportionality As Components of the War Against Terrorism: Is the U.S. Judiciary in Self-Imposed Exile?, 7 J. MONEY LAUNDERING 245 (2004).

292. Complaint regarding NSA <http://www.aclu.org/pdfs/safefree/nsacomplaint.011706.pdf>. The ACLU filed the suit in the United States District Court for the Eastern District of Michigan—the same court that decided *Keith*. See *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297 (1972).

293. 438 F. Supp. 2d 754 (E.D. Mich. 2006).

294. *Id.* at 782.

295. *Id.*

296. See *id.* at 775.

297. *Id.* at 769-71.

298. *ACLU*, 438 F. Supp. 2d at 777-78.

to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.”²⁹⁹ The Fourth Amendment “requires reasonableness in all searches.”³⁰⁰ Congress spoke in establishing the FISA; therefore, FISA lawfully provided the executive branch with numerous circumstances to conduct warrantless surveillance in times of emergency.³⁰¹ However, the court held that Congress had not spoken with respect to the immensely invasive nature of the NSA program which was deemed objectively unreasonable in relation to the larger context of the body of law.³⁰²

In addition to addressing the violations of Fourth Amendment rights, the court also held that the NSA program unconstitutionally interfered with the plaintiff’s First Amendment right to free expression.³⁰³ The court, strengthened by the earlier cases examining similar governmental regulation of protected speech,³⁰⁴ noted that a governmental action to regulate speech may be “justified only upon showing of a compelling governmental interest; and that the means chosen are least restrictive. . . .”³⁰⁵ FISA had already lawfully provided the executive branch with the power to engage in warrantless surveillance, and therefore, the NSA program was not the least restrictive means of accomplishing national security goals.³⁰⁶

The separation of power issue, the executive weapon for marginalizing Article III review post 9/11, also invoked a judicial response. The court noted that the key to a free government is the lodging of the control of

299. *Id.* at 775 (citing *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 315-17 (1972)).

300. *Id.*

301. *Id.*

302. *See id.*

303. *ACLU*, 438 F. Supp. 2d at 776.

304. Judge Taylor was very mindful that national security cases often present a mix of Fourth and First Amendment concerns. *Id.* Her recognition of the policy articulated in *Keith* is apt:

Though the investigative duty of the executive may be stronger in [national security] 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.

Id. (citing *United States v. U.S. Dist. Court*, 407 U.S. 297, 313-14 (1972)).

305. *ACLU*, 438 F. Supp. 2d at 776.

306. *Id.*

emergency powers outside the executive branch.³⁰⁷ Recalling the seminal teachings of Justice Jackson in *Youngstown Sheet and Tube Co. v. Sawyer*,³⁰⁸ the court recognized that when the President acts in contravention to the will of Congress, his power is at a minimum and he may only rely on his inherent constitutional power.³⁰⁹ Because the President squarely defied the will of Congress as expressed through FISA, the President's power was at its lowest ebb.³¹⁰

As an alternative basis of support, that the President was actually acting in accord with Congress, the government argued that Congress implicitly authorized the NSA program with the passage of AUMF.³¹¹ The court, however, was not persuaded.³¹² Noting that the rules of statutory construction require that the specific statutes govern those of general applicability, the court held that the highly specific commands of FISA overrule any suggestion of legality raised by the AUMF.³¹³

Because the President lacked congressional authorization to effectuate the NSA program, the court acknowledged that any legal justification for the NSA program would have to stem directly from the President's inherent power under the Constitution.³¹⁴ The court further noted that the executive branch is itself a creature of the Constitution, and therefore constrained by the limits of that document. As such, the court concluded that the actions taken by the executive must comport to the First and Fourth Amendments.³¹⁵ Since the highly invasive nature of the NSA program violated those amendments, the President lacked inherent authority to authorize the program.³¹⁶ In short, the NSA program was in direct violation of the liberties contained in the Constitution. Mindful of those liberties, the court concluded: "It was never the intent of the Framers to give the President such unfettered control, particularly where his actions blatantly disregard the parameters clearly enumerated in the Bill of Rights."³¹⁷ With that, the court ordered an immediate halt to the program.³¹⁸

307. *Id.* at 778.

308. 343 U.S. 579 (1952).

309. *ACLU*, 438 F. Supp. 2d at 777.

310. *Id.* at 778.

311. *Id.* at 779.

312. *Id.*

313. *Id.*

314. *ACLU*, 438 F. Supp. 2d at 776.

315. *Id.* at 781.

316. *Id.*

317. *Id.* at 771

318. *Id.* at 782.

The President has appealed the ruling; and the controversy is far from resolved.³¹⁹ The opinion of Judge Taylor has been assailed, and some critics argue it is thinly reasoned.³²⁰ To resolve the matter, the Bush Administration continues to request Congress grant explicit authorization for the NSA program.³²¹

Judge Taylor's opinion may be overturned; however, Judge Taylor did more than just draft an opinion reaffirming the right of the people to be free from unreasonable search and seizure. She demonstrated that there are still those who not only read the Constitution of the United States, but also are willing to put their educated findings on paper for all to review.

The post-9/11 attempts by the Bush administration to marginalize judicial review under Article III of the U.S. Constitution have been met with considerable judicial opposition.³²² Judge Taylor is not alone in her fidelity to her oath. Federal judges from all corners of the nation are now involved as partners in ensuring that the republic stands with the Constitution in tact. Judge Taylor reaffirms a basic principle of our Constitution: the Bill of Rights is not a suicide pact.³²³

Judge Taylor's opinion represents an acknowledgment of the importance of public review. Learned Hand noted long ago that Article III is not enough; the people must learn the difference between rights and doublespeak.³²⁴ As Learned Hand put it: "Liberty lies in the hearts of men and women; if it dies there, no constitution, no law, no court can save it."³²⁵

319. See Dan Eggan & Dafna Linzer, *Judge Rules Against Wiretaps*, WASH. POST, Aug. 18, 2006, at A1.

320. *Id.*

321. *Id.*

322. See, e.g., *Hepting v. AT&T Corps.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006); *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006); *Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006).

323. See Baldwin, *supra* note 270, at 245.

324. See generally Timothy Lynch, *Doublespeak and the War on Terrorism*, Cato Inst. Briefing Papers No. 98, Sept. 6, 2006.

325. *Id.* at 11; Learned Hand, *The Spirit of Liberty*, in *SPIRIT OF LIBERTY: PAPER AND ADDRESSES OF LEARNED HAND 189-90* (2d ed. 1953).