

FISA's Future: An Analysis of Electronic Surveillance in Light of the Special Needs Exception to the Fourth Amendment

Justin W. Whitney*

*In God we trust. All others bring data.*¹

I. INTRODUCTION

In August 2006, Pakistan's military intelligence, the Inter Services Intelligence (ISI) alerted Britain's counter-intelligence, MI5, of a plot to blow up several U.S.-bound jets using remote-controlled liquid explosives.² Meanwhile in London, British police arrested twenty-four suspects, most of who were British citizens of Pakistani origin.³ Fortunately, the U.K. terror plot was narrowly foiled in the last hour.⁴ But, who foiled it?

At least one commentator has suggested the unraveling of the U.K. plot was an orchestrated staging between the ISI, MI5, and the Central Intelligence Agency (CIA).⁵ Best-selling author and Economics Professor Michel Chossudovsky suggests that the ISI is presently running and supporting terrorist camps in Pakistan.⁶ The Council on Foreign Relations reports that the ISI provides financial assistance to the terrorist organization Jaish-e-Muhammad (Army of Mohammed).⁷ The Associated Press linked Jaish-e-Muhammad to masterminding the death of 190 people in a train bombing in Mumbai as recently as July 2006.⁸ In addition, investigations traced funding for the 9/11 terrorist attack to the leader of the ISI.⁹

Chossudovsky theorizes that the tip-off was merely a smoke-screen

* B.S. 2002, University of Kansas; J.D. 2007, Washburn University School of Law.

1. DAVID H. HILDEBRAND & R. LYMAN OTT, STATISTICAL THINKING FOR MANAGERS 1 (1998).

2. Michel Chossudovsky, *The Foiled UK Terror Plot and the "Pakistani Connection,"* GLOBAL RESEARCH, Aug. 14, 2006, <http://www.globalresearch.ca/index.php?context=va&aid=2960>. See also Alan Cowell, Dexter Filkins, & Mark Mazzetti, *Threats and Responses: The Investigation; Suspect Held in Pakistan is Said to Have Ties to Qaeda*, N.Y. TIMES, Aug. 12, 2006, at A1.

3. Cowell, *supra* note 2, at A1.

4. *Id.*

5. See Chossudovsky, *supra* note 2.

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

in which ISI demonstrated their commitment to transforming into a reformed, anti-terrorism agency, while in reality high-level officials, or at least rogue elements within, continue to support terrorism.¹⁰ Fortunately, national security does not depend solely on hand-outs from terrorist-supporting organizations. Rather, our government operates a labyrinth of intelligence gathering practices designed to prevent attack from foreign powers. The nerve center of this intelligence network is the National Security Agency (NSA).

The NSA's role in unraveling the U.K. terror plot remains classified. If, however, the NSA's controversial Terrorist Surveillance Program (TSP) did play a key role in thwarting the attack, it is now unclear whether the TSP will survive to help deter future attacks. Merely six days after the unraveling of the U.K. terror plot, a federal judge issued an injunction against the TSP and declared it unconstitutional.¹¹

The constitutionality of the TSP has gained media attention since the New York Times released details of the TSP in December 2005.¹² In response to the court decision and the media controversy, on January 17, 2007, Attorney General Alberto Gonzalez announced that the NSA's warrantless surveillance, generally referred to as the TSP, will cease and the NSA will now conduct future surveillance with court approval under the Foreign Intelligence Surveillance Act of 1978 (FISA).¹³

Opponents of warrantless surveillance argue that Congress strictly limited the means for conducting it by enacting FISA. Critics maintain the TSP lacks congressional approval similar to the Supreme Court ruling that the President's military tribunals lacked congressional approval in *Hamdan v. Rumsfeld*.¹⁴ This article suggests that analyzing warrantless executive surveillance in terms of congressional approval is problematic because it raises separation of powers concerns.

Both the Administration and critics cite statutory arguments for and against warrantless surveillance. Statutory arguments are also problematic because the *Hamdan* decision left the Supreme Court in a position where it cannot address the statutory authority for the TSP without contradicting precedent. As this article explains, whether the TSP com-

10. *Id.*

11. *ACLU v. NSA*, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006), *rev'd*, *ACLU v. NSA*, No. 06-2095/2140 (6th Cir. July 6, 2007) (vacating the district court's order upon a finding that all plaintiffs lacked standing and remanding with instructions that the action be dismissed).

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

13. Eric Lichtblau & David Johnston, *Court to Oversee U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007, at A1. FISA originated in response to a congressional investigation into surveillance abuses by the intelligence community. Adam Burton, *Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381, 386 (2006). In 1976, reports by the Church Committee—headed by Senator Frank Church—detailed widespread intelligence abuse and urged Congress to enact legislation to keep the abuses in check. *Id.* Among the abuse was a 1963 decision by Attorney General Robert Kennedy to wiretap Dr. Martin Luther King, Jr. *Id.*

14. 126 S. Ct. 2749 (2006).

plies with FISA turns on whether Congress granted the President authority to deviate from FISA in passing the Authorization for the Use of Military Force (AUMF). In *Hamdi v. Rumsfeld*,¹⁵ the Court determined that the AUMF was sufficiently broad to grant the President implicit powers incident to war.¹⁶ Yet the *Hamdan* Court interpreted the AUMF as too narrow to deviate from congressional approval.¹⁷ The inconsistent interpretations of the AUMF render it inadequate as a means for analyzing the constitutionality of executive surveillance.

In the past, the state secrets doctrine often arose in cases involving executive surveillance. Under that doctrine, evidence related to national security is immune from discovery.¹⁸ However, a recent increase in media coverage of national security matters has swallowed the doctrine's protections.¹⁹ The growth in media exposure has rendered the state secrets doctrine unsuitable for an analysis of warrantless surveillance. Like the attempts to analyze authority under FISA and to interpret the AUMF, a decision premised on the state secrets doctrine is inadequate to fully resolve the complexities of warrantless surveillance.

This article proposes an alternative analysis using the special needs exception to the Fourth Amendment. Special needs of law enforcement sometimes permit suspicionless searches. Viewed from this perspective, courts could use statistical forecasting to measure whether continued surveillance is necessary to address the special needs of law enforcement. Part V suggests a forecasting model wherein past data may prove that after a specified duration of surveillance without success, the probability of continued surveillance generating probable cause becomes too remote to justify a special needs exception to the Fourth Amendment. An analysis based on statistical certainties could foreclose any need for courts to rule on executive surveillance with an ad-hoc interpretation of the Constitution.

II. BACKGROUND INFORMATION

A. *The National Security Agency (NSA) and Data-Mining*

The NSA is a distinct agency within the Department of Defense (DOD) that performs intelligence gathering under the control of the Secretary of Defense.²⁰ NSA surveillance of individuals outside the U.S.

15. 542 U.S. 507 (2004).

16. *Id.* at 518-19.

17. *Hamdan*, 126 S. Ct. at 2774.

18. *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989).

19. See *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 991-92, 994 (N.D. Cal. 2006) (refusing to apply the state secrets doctrine to information that has already been reported in the media).

20. Department of Defense Directive No. 5100.20 (Dec. 23, 1971).

is not subject to Fourth Amendment limitations.²¹ Data-mining is the process of using statistical science and modeling to find relationships within a data set.²² In the intelligence sector, agencies sort through large databases of public and private information to find relationships within the data.²³ Data-mining is not limited to national security matters.²⁴

In 2004, fifty-two federal agencies reported using data-mining to the Government Accounting Office.²⁵ Among the reported uses for data-mining were improving service, detecting waste, and managing human resources.²⁶ An example of government data-mining is the Multistate Anti-Terrorism Information Exchange System (MATRIX). MATRIX stores and analyzes information among multiple departments of state and federal law enforcement.²⁷ The Bush Administration created MATRIX in response to the 9/11 attacks.²⁸ MATRIX contains drivers license data, criminal records, and photos.²⁹

The NSA is actively involved in data-mining and is reportedly tracking millions of phone calls to the businesses and residences of American citizens.³⁰ The agency rarely listens to the calls, but analyzes the calling patterns to detect potential terrorism.³¹ Since September 11, 2001, the NSA has had access to the records of almost every telephone call in the United States.³² The data allows the NSA to track how suspected terrorists interact with each other.³³

An example of an NSA data-mining project is the Terrorism Information Awareness (TIA) program. TIA was a prototype of a large-scale data-mining network with capability to search and identify patterns relevant to fighting terrorism.³⁴ The prototype also had language translation and decision-making capabilities.³⁵ The program's goal was to enable the DOD to systematically exploit data to combat terrorism.³⁶

The architects of TIA realized that information on American citi-

21. David Alan Jordan, *Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice Over Internet Protocol*, 47 B.C. L. REV. 1, 13-14 (2006).

22. U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 1 (2004).

23. *Id.* at 6.

24. *Id.* at 7.

25. *Id.*

26. *Id.*

27. *Id.* at 5.

28. *Id.*

29. *Id.*

30. Julie Hirschfeld Davis, *Bush Defends Spy Program*, BALT. SUN, May 12, 2006, at 1A.

31. Eric Lichtblau & Scott Shane, *Bush is Pressed over New Report on Surveillance*, N.Y. TIMES, May 12, 2006, at A1.

32. *Id.*

33. *See id.*

34. U.S. DEP'T OF DEFENSE, REPORT TO CONGRESS REGARDING THE TERRORIST INFORMATION AWARENESS PROGRAM 1 (2003).

35. *Id.*

36. *Id.* at 2.

zens would inevitably enter the system.³⁷ Thus, the prototype contemplated the design of comprehensive internal controls to protect individual privacy rights.³⁸ The internal controls include an auditing function that maps a trail of each user who accesses the network and a feature for keeping data anonymous until legal approval is granted to inquire further into the data.³⁹ The network benefited from evolving technology programs to compile its data such as the Human Identification at a Distance (HumanID) program and the Next Generation Face Recognition (NGFR) program.⁴⁰

Congress cut off funding for the TIA, but there is no indication that the NSA has given up on data-mining to fight terrorism.⁴¹ In May 2006, the NSA disclosed that it is compiling phone records from the major U.S. telecommunications firms to aid in fighting terrorism.⁴² Phone records may not be the extent of the NSA's data-mining. Databases can be comprised of bank transactions, airline ticket purchases, Google internet searches, and credit card purchases. For example, the Department of the Treasury maintains a database called the Financial Crimes Enforcement Network.⁴³ Unusually suspicious transactions, such as international funds transfers or cash deposits exceeding \$10,000, are flagged, stored, and shared with multiple law enforcement agencies.⁴⁴

B. The Terrorist Surveillance Program (TSP)

Media reports and recent cases have unearthed the details of the TSP. In *Hepting v. AT&T Corp.*,⁴⁵ the plaintiffs sought a preliminary injunction of NSA wiretapping alleged to be taking place at AT&T's

37. *Id.* at 4.

38. *Id.*

39. *Id.*

40. The HumanID program utilizes biometric identification technology. DARPA Fact File: A Compendium of DARPA Programs, http://www.darpa.mil/body/news/2002/darpa_fact.html (last visited Sept. 25, 2007). Biometric technology recognizes patterns in the manner a person walks, their fingerprints, and facial features from a distance and compiles these patterns into a biometric signature used to identify a suspect. *Id.* The Defense Advanced Research Projects Agency (DARPA) contracted with Visionics Corporation to implement the program. *DARPA Extends Visionics Participation in Human ID at a Distance Program: Current Year Contract Calls for Nearly \$1 Million in Additional Funding*, MACHINE VISION ONLINE, Apr. 10, 2002, <http://www.machinevisiononline.org/public/articles/archivedetails.cfm?id=1061>. Visionics, a global leader in identification security products, invented a system called FaceIt, which automatically matches photos of suspects on watch lists to images on closed circuit television cameras. *Id.*

41. Michael J. Sniffen, *Congress Limits Pentagon Surveillance: Parts of Project Continue in Secret*, HOUSTON CHRON., Sept. 26, 2003, at A15.

42. Arshad Mohammed & Terence O'Hara, *NSA Program Further Blurs Line on Privacy*, WASH. POST, May 13, 2006, at D1. The most threatening signal intelligence is disseminated to the Director of Central Intelligence. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 254 (2004). CIA management prioritizes six to eight of the most critical threats on any given day and compiles them into the President's Daily Brief, which is only shared with a few high-level officials. *Id.*

43. Mohammed & O'Hara, *supra* note 42, at D1.

44. *Id.*

45. 439 F. Supp. 2d 974 (N.D. Cal. 2006).

San Francisco office.⁴⁶ The plaintiffs supported the motion with documents obtained by Mark Klein, a former employee of AT&T.⁴⁷ Klein described witnessing workers constructing a new room next to a switch room for wiretapping at the direction of an NSA agent.⁴⁸

The *Hepting* court began its analysis by recognizing admissions from President Bush's radio address on December 17, 2005.⁴⁹ In that address, the President admitted that in the weeks after September 11, 2001, he "authorized the National Security Agency . . . to intercept the international communications of people with known links to al Qaeda and related terrorist organizations."⁵⁰ He also said, "Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks."⁵¹ President Bush further revealed that the Attorney General reviews the surveillance activities every forty-five days and that leaders in Congress are updated on the program.⁵² The court also took judicial notice of a public statement President Bush made on May 11, 2006.⁵³ He said that the government's "international activities strictly target al Qaeda and their known affiliates," and that the government is "not mining or trolling through the personal lives of millions of innocent Americans."⁵⁴

The court also took notice of Attorney General Alberto Gonzalez's comments on the subject.⁵⁵ Gonzalez revealed in a December 19, 2005 press briefing that the surveillance program intercepts

contents of communications where . . . one party to the communication is outside the United States . . . [and the government 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.⁵⁶

Gonzalez further stated, "This [program] is not about wiretapping everyone. This is a very concentrated, very limited program focused at gaining information about our enemy."⁵⁷ A released publication from the Department of Justice (DOJ) explains that the TSP only conducts surveillance when one recipient is located abroad.⁵⁸

46. *Id.* at 979.

47. *Id.*

48. *Id.* at 989.

49. *Id.* at 987.

50. President George W. Bush, Presidential Radio Address (Dec. 17, 2005) (transcript available at <http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html>).

51. *Id.*

52. *Id.*

53. *Hepting*, 439 F. Supp. 2d at 987.

54. President George W. Bush, Public Statement (May 11, 2006) (transcript available at <http://www.whitehouse.gov/news/releases/2006/05/20060511-1.html>).

55. *Hepting*, 439 F. Supp. 2d at 987.

56. Alberto Gonzalez, U.S. Attorney Gen., Press Briefing (Dec. 19, 2005), (transcript available at <http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html>).

57. *Id.*

58. Press Release, U.S. Dep't of Justice, The NSA Program to Detect and Prevent Terrorist Attacks: Myth v. Reality 2 (Jan. 27, 2006), available at <http://www.usdoj.gov/opa/documents/>

The court also referenced a May 11, 2006, article in *USA Today* reporting that BellSouth Corp., Verizon, and AT&T had provided telephone records to the NSA for analyzing calling patterns.⁵⁹ The article contained a statement from the attorney for Qwest Communications' CEO Joseph Nacchio.⁶⁰ The statement indicated that the government requested Nacchio to reveal private phone records, but he refused when the officials indicated no intention to use the process provided by the FISA courts.⁶¹

III. LEGAL FRAMEWORK

A. Constitutional Aspect

1. Fourth Amendment and the *Keith* Case

Article II, section 1 of the Constitution imposes a duty on the President to "preserve, protect and defend the Constitution of the United States."⁶² Because of that duty, the Supreme Court has stated that the President has implicit authority to protect our system of government from subversion.⁶³ The Fourth Amendment, however, restricts the President's duty to protect the nation's security and guarantees by protecting U.S. persons from unreasonable searches and seizures absent a warrant based on probable cause.⁶⁴

The conflict between national security and the Fourth Amendment unfolded in *United States v. U.S. District Court (Keith)*.⁶⁵ In the *Keith* case, the defendant allegedly bombed the CIA office in Ann Arbor, Michigan with dynamite.⁶⁶ The defense sought disclosure of wire-tap evidence obtained against the defendant.⁶⁷ The Attorney General admitted to the court that he had approved government agents to conduct warrantless electronic surveillance on the defendant as necessary to guard against "attempts of domestic organizations to attack and sub-

nsa_myth_v_reality.pdf (stating "[c]ommunications are only intercepted if there is a reasonable basis to believe 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").

59. *Hepting*, 439 F. Supp. 2d at 988 (citing Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006).

60. *Id.*

61. *Id.*

62. U.S. CONST. art. II, § 1.

63. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 310 (1972).

64. U.S. CONST. amend IV.

65. 407 U.S. 297, 299 (1972).

66. *Id.* Just five years earlier, the Supreme Court held that surveillance on private telephone conversations without a warrant was unreasonable under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 359 (1967).

67. *Keith*, 407 U.S. at 299-300.

vert” the government.⁶⁸ The Supreme Court set out to define the limits of the Presidential power to protect national security with warrantless domestic wire-tapping, a practice that the Court recognized the executive branch had conducted for at least twenty-five years.⁶⁹

The *Keith* Court recognized the President’s implicit constitutional power to conduct surveillance on foreign powers and on domestic powers.⁷⁰ The Court, however, held that warrantless surveillance over purely domestic powers violates the Fourth Amendment.⁷¹ The Court made clear that its holding did not limit the President’s power to conduct surveillance “with respect to activities of foreign powers or their agents.”⁷² Thus, the Court limited the holding to the President’s constitutional power to conduct surveillance over domestic powers meaning, “composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies.”⁷³ *Keith*’s limited holding did not answer whether the President has Article II power to conduct electronic surveillance on citizens possessing a significant connection to a foreign power or its agents.⁷⁴

2. The National Security Exception to the Fourth Amendment

Keith’s limited holding did not disturb the concept of a national security exception to the Fourth Amendment that justifies warrantless electronic surveillance when domestic citizens communicate with foreign powers or their agents.⁷⁵ Every federal appellate court that has addressed this type of surveillance by the executive branch has upheld the conduct as constitutional.⁷⁶ *United States v. Hoffman*⁷⁷ is an example of judicial reluctance to prohibit executive surveillance.

In *Hoffman*, a criminal defendant moved for disclosure of five incriminating conversations the government caught on tape with electronic surveillance.⁷⁸ The government obtained four of the conversations during surveillance of purely domestic organizations to gain information about threats posed by the domestic organization.⁷⁹ The government gathered the fifth conversation during surveillance con-

68. *Id.* at 300.

69. *Id.* at 310.

70. *Id.* at 309 n.8.

71. *Id.* at 320-22.

72. *Id.* at 321-22.

73. *Id.* at 309 n.8.

74. *Id.* at 321-22.

75. See Michael A. DiSabatino, Annotation, *Construction and Application of “National Security” Exception to Fourth Amendment Search Warrant Requirement*, 39 A.L.R. FED. 646, § 2a (1978).

76. Press Release, *supra* note 58, at 1.

77. 334 F. Supp. 504 (D.C. Cir. 1971).

78. *Id.* at 505.

79. *Id.* at 506.

ducted to intercept foreign intelligence relevant to national security.⁸⁰ The court held that the President's inherent authority over foreign affairs entitles the executive branch to utilize domestic warrantless surveillance when necessary to obtain foreign intelligence critical to national security.⁸¹ Applied to the facts of the case, the warrantless surveillance of the purely domestic organizations violated the Fourth Amendment because the surveillance was not related to national security.⁸² In other words, the court held that the President may constitutionally conduct warrantless surveillance when the purpose is linked to gathering foreign intelligence on national security.

3. The Special Needs Exception to the Fourth Amendment

Law enforcement can deviate from FISA and remain within constitutional bounds through the special needs exception to the Fourth Amendment.⁸³ While surveillance related to general crime prevention requires a warrant under the Fourth Amendment, courts relax the warrant requirement if necessary to monitor a specific threat.⁸⁴ The special needs exception to the Fourth Amendment constitutionally authorizes the President to conduct warrantless surveillance in response to specific threats from foreign powers.⁸⁵

In *United States v. Truong*,⁸⁶ the United States Court of Appeals for the Fourth Circuit addressed the President's constitutional authority to monitor the specific threat that foreign powers pose within the U.S.⁸⁷ The government monitored David Truong, a Vietnamese citizen, with electronic surveillance upon suspicion that he was transmitting classified information to Vietnam.⁸⁸ The government bugged Truong's apartment and phone for almost one year continuously without court authorization.⁸⁹ Upon his conviction for espionage, Truong argued that the surveillance violated the Fourth Amendment.⁹⁰ The *Truong* court interpreted *Keith* to imply that the President can constitutionally conduct warrantless surveillance for foreign intelligence purposes.⁹¹ It held that the need for foreign intelligence information is too great to justify a uni-

80. *Id.*

81. *Id.* at 507-08.

82. *Id.* at 508.

83. *In re Sealed Case*, 310 F.3d 717, 745 (FISA Ct. Rev. 2002).

84. *Id.* at 742-44.

85. See *id.* at 746; see also Katherine Wong, *Recent Development: The NSA Terrorist Surveillance Program*, 43 HARV. J. ON LEGIS. 517, 523 (2006) (explaining the constitutional arguments for and against the Terrorist Surveillance Program (TSP)).

86. 629 F.2d 908 (4th Cir. 1980).

87. *Id.* at 911-12.

88. *Id.* at 912.

89. *Id.*

90. *Id.*

91. *Id.* at 913-14.

form warrant requirement.⁹² Such a requirement would frustrate the executive's ability to counter foreign threats.⁹³ The *Truong* court recognized that countering foreign threats necessitates speed and secrecy.⁹⁴ The hurdles of a warrant requirement limit the executive branch's flexibility and increase the time required to respond to a foreign threat.⁹⁵ According to the court, a warrant requirement would increase the chance of leaking sensitive executive information.⁹⁶

Equally important to the *Truong* court was recognition that the executive branch has expertise in surveillance decisions that the judiciary lacks.⁹⁷ District courts lack the knowledge to assess and weigh the importance of foreign intelligence information relevant to a probable cause determination.⁹⁸ This analysis is better left in the hands of the executive branch, comprised of the intelligence community and military, which is better equipped to assess external threats.⁹⁹ Putting aside the impracticalities of a warrant requirement for foreign surveillance, the court recognized that the Constitution mandates the executive branch to be the "pre-eminent authority in foreign affairs."¹⁰⁰ In upholding *Truong's* conviction, the court stated that separation of powers demands that conducting domestic security surveillance is the President's principal responsibility.¹⁰¹

Truong distinguished between foreign intelligence surveillance and crime investigation surveillance.¹⁰² If the primary purpose of surveillance was to gather foreign intelligence, then the special needs exception was triggered, and the warrant requirement was relaxed.¹⁰³ If the primary purpose was criminal prosecution, the surveillance was subject to the usual warrant requirements.¹⁰⁴ The *Truong* court drew a bright line as to when the purpose of surveillance becomes primarily criminal.¹⁰⁵ Moreover, the *Truong* court left an impression in law enforcement that the surveillance became primarily criminal at the moment the agency's criminal division assumed the lead role.¹⁰⁶ This framework resulted in the FBI transferring criminal investigations to other government agencies to ensure there was no overlap between criminal and foreign intelli-

92. *Id.* at 914.

93. *Id.* at 913.

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.* at 913-14.

99. *Id.*

100. *Id.* at 914.

101. *Id.*

102. *Id.* at 915.

103. *Id.*

104. *Id.*

105. *Id.*

106. *In re Sealed Case*, 310 F.3d 717, 742-43 (FISA Ct. Rev. 2002).

gence purposes that would require a warrant.¹⁰⁷ The *Truong* test resulted in a compartmentalized approach that erected a wall within the Justice Department.¹⁰⁸

This wall analogy surfaced in testimony before Congress regarding the failure to prevent the 9/11 attack.¹⁰⁹ A New York FBI agent testified that senior FBI officials prohibited agents from initiating a criminal investigation into two of the 9/11 hijackers because they feared a criminal investigation would require a warrant.¹¹⁰ Out of frustration, one agent infamously predicted in a letter to FBI headquarters: "Someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' . . . [T]he biggest threat to us now, [Usama Bin Laden], is getting the most 'protection.'"¹¹¹ The holding from *In re Sealed Case*¹¹² criticized the compartmentalized approach from *Truong*.¹¹³

Recently, the Supreme Court has indicated that the threat of terrorism might be a valid special needs exception to the Fourth Amendment. In *City of Indianapolis v. Edmond*,¹¹⁴ the Court invalidated a suspicionless highway checkpoint created to detect drug transportation.¹¹⁵ The Court ruled that the primary purpose of drug prosecution was insufficient to justify a suspicionless search.¹¹⁶ Rather, suspicionless searches require a purpose beyond criminal prosecution such as protecting citizens against special hazards like unsafe drivers.¹¹⁷ According to the Court, thwarting an imminent terrorist plot would justify a suspicionless search.¹¹⁸

4. The State Secrets Doctrine

Lawsuits involving the NSA typically turn on the state secrets doc-

107. *Id.* at 743 n.27.

108. *Id.* at 743.

109. *The Malaysia Hijackers and September 11: J. Hearing Before the S. and H. Select Intelligence Comms.*, 107th Cong. 56-7 (2002) (prepared statement of New York special agent of the FBI).

110. *See id.*

111. *Id.* On July 24, 2001, an unidentified FBI intelligence analyst began tracking suspected terrorist Khalid al Mihdhar based on links connecting him to the October 2000 bombing of the U.S.S. *Cole*. THE 9/11 COMMISSION REPORT, *supra* note 42, at 151, 266, 268, 270. A criminal investigator within the FBI who had specialized knowledge and experience in tracking down al Qaeda suspects approached the analyst. *Id.* at 271. The intelligence analyst, following advice from the FBI's National Security Law Unit, blocked the criminal investigator's access to her reports because they contained NSA information available only for intelligence purposes rather than criminal investigation. *Id.* The withholding of information excluded an experienced al Qaeda tracker from the search for Khalid al Mihdhar. *Id.* On September 11, 2001, Mihdhar boarded American Airlines Flight 77 in seat 12B bound from Washington Dulles to Los Angeles and was identified as one of the five hijackers responsible for its later crash into the Pentagon at 530 miles per hour. *Id.* at 8-10.

112. 310 F.3d 717 (FISA Ct. Rev. 2002).

113. *Id.* at 744.

114. 531 U.S. 32 (2000).

115. *Id.* at 34, 48.

116. *Id.* at 47 n.2, 48.

117. *Id.* at 41.

118. *Id.* at 44.

trine. “The state secrets privilege is a common law evidentiary rule that protects information from discovery when disclosure would be inimical to the national security.”¹¹⁹ The Supreme Court crafted a precursor to the state secrets privilege in *Totten v. United States*.¹²⁰ In *Totten*, the estate of a former spy sought a breach of contract for payment of an express espionage agreement with the President.¹²¹ The *Totten* Court found it a violation of public policy to allow a party to bring suit on a government contract based on secrets essential to national security.¹²²

The privilege emerged in *United States v. Reynolds*¹²³ where families of civilians killed by a downed military aircraft sought discovery of the cause of the accident¹²⁴ The government claimed that producing documents regarding the accident would reveal state and military secrets.¹²⁵ The *Reynolds* Court went on to state that when a court finds, “from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged.”¹²⁶

B. Statutory Aspect

1. The Foreign Intelligence Surveillance Act of 1978 (FISA)

FISA lists various alternatives for the President to authorize the Attorney General to conduct surveillance for gathering foreign intelligence information.¹²⁷ The first option is § 1802, which permits surveillance for up to one year without a court order, provided the Attorney General certifies certain prerequisites.¹²⁸ The Attorney General must certify that the surveillance is directed at communications “used exclusively between or among foreign powers” and that “there is no substantial likelihood” of capturing communications of a U.S. person.¹²⁹ A

119. *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989).

120. 92 U.S.105 (1875).

121. *Id.* at 105-06.

122. *Id.* at 107. The intestate heir of William A. Lloyd, a deceased spy, brought suit alleging the existence of a contract between President Lincoln and Lloyd in 1861 to spy on confederate troop movement. *Id.* at 105. Lloyd was allegedly instructed to travel south in an attempt to ascertain the number of confederate soldiers moving northward. *Id.* at 105-06. Lloyd managed to submerge himself within the confederate troops and transmit information to the President. *Id.*

123. 345 U.S. 1 (1953).

124. *Id.* at 2-3.

125. *Id.* at 4-5.

126. *Id.* at 10.

127. 50 U.S.C. §§ 1801-63 (2000 & Supp. III 2005).

128. *Id.* § 1802.

129. *Id.* § 1802(a)(1)(A)-(B) (2000). On August 3, 2007, the Senate passed the Protect America Act to amend certain FISA provisions. Lara Jakes Jordan, *Senate Passes Bush Terrorism Spy Bill*, CINCINNATI POST, Aug. 4, 2007, at A. Specifically, the Act proposes to amend the certification prerequisites of §1801(a). Protect America Act, S. 1927, 110th Cong. § 2 (2007). The proposed amendment requires certification of procedures to ensure that the intelligence gathered concerns “persons reasonably believed to be located outside the United States.” *Id.* The amendment also mandates

“[f]oreign power” generally means a foreign government or a group conducting international terrorism.¹³⁰ A “U. S. person” generally means a U.S. citizen or lawful alien.¹³¹ The requirement of avoiding communications of U.S. persons makes this avenue the most restrictive option for the government to obtain surveillance in compliance with FISA.

The second option is § 1805, which permits the Attorney General to obtain a court order approving the surveillance based on a finding of probable cause.¹³² A third option is an exception under § 1805(f) wherein seventy-two hours of emergency surveillance can be conducted provided notice is given to the FISA court.¹³³ The fourth option is less restrictive than both §§ 1802 and 1805. Section 1842 permits the Attorney General to conduct surveillance pursuant to a court order but without a showing of probable cause.¹³⁴ The court order generally grants upon a certification by the Attorney General that foreign intelligence information is likely to be obtained and relates to protecting against international terrorism.¹³⁵ Unless the Attorney General obtains an extension, the order will expire in ninety days.¹³⁶

Stringent FISA limitations ensure the government fulfills constitutional requirements while gathering foreign intelligence within the U.S.¹³⁷ FISA constrains a significant amount of surveillance opportunities because much of the world's data is shuttled through the U.S.¹³⁸ Approximately one percent of international long-distance communications transmit through satellites, and the rest pass through undersea fiber-optic cables.¹³⁹ Even calls that originate and terminate outside the U.S. route through America on the lines of domestic backbone providers, making wire tapping of international data feasible without tapping data lines abroad.¹⁴⁰

FISA has no relevance to surveillance conducted on non-citizens outside the U.S., because those individuals are not entitled to Fourth Amendment protection.¹⁴¹ In these situations, the government is not

certification that the intelligence acquisition requires cooperation from a communication services provider. *Id.* The Act expires in 180 days and is only a temporary solution while Congress debates more permanent amendments. *Id.* § 6. President Bush signed the bill into law on August 6, 2007. James Risen, *Bush Signs Bill to Widen Legal Reach for Wiretaps: No Warrants Needed for Overseas Calls*, INT'L HERALD TRIB., Aug. 7, 2007, at 1.

130. 50 U.S.C. § 1801(a) (2000).

131. *Id.* § 1801(i).

132. *Id.* § 1805(a).

133. *Id.* § 1805 (f).

134. *See id.* § 1842 (2000 & Supp. III 2005).

135. *Id.* § 1842(c)(2) (2000).

136. *Id.* § 1842(e).

137. Jordan, *supra* note 21, at 13.

138. Declan McCullagh & Anne Broache, *NSA Eavesdropping: How It Might Work*, CNET NEWS.COM, Feb. 7, 2006, http://news.com.com/NSA+eavesdropping+How+it+might+work/2100-1028_3-6035910.html (statement of Jim Hayes, President of Fiber Optic Association).

139. *Id.*

140. *Id.*

141. Jordan, *supra* note 21, at 13-14; *see also* United States v. Verdugo-Urquidez, 494 U.S. 259,

subject to any rules regarding electronic surveillance. This lack of regulation creates the possibility for secret programs like the rumored intelligence project ECHELON—a secret intelligence gathering network reportedly capable of intercepting radio and data communication across the planet using satellites.¹⁴² ECHELON makes global intercepts of everything from cellular phones to baby monitors.¹⁴³

2. Authorization for Use of Military Force (AUMF)

On September 18, 2001, a joint resolution of Congress authorized the President to “use all necessary and appropriate force” against those he determines aided in the 9/11 terrorist attack.¹⁴⁴ The Bush Administration offers that the AUMF and FISA form consistent links in a chain authorizing the TSP.¹⁴⁵ FISA permits surveillance as provided by congressional authorization.¹⁴⁶ Congress in turn authorized surveillance under the AUMF.¹⁴⁷ This analysis gained favor by the Supreme Court in the case of *Hamdi v. Rumsfeld*.¹⁴⁸

3. *Hamdi v. Rumsfeld*

The Supreme Court interpreted the AUMF in *Hamdi*. Yaser Esam Hamdi was an American citizen residing in Afghanistan.¹⁴⁹ In 2001, the Northern Alliance captured Hamdi during a battle with the Taliban and turned Hamdi over to the U.S. military.¹⁵⁰ Hamdi was allegedly captured holding a Kalishnikov assault rifle.¹⁵¹ Hamdi’s father filed a writ of habeas corpus in federal district court on behalf of his son.¹⁵² Hamdi claimed that his detention violated 18 U.S.C. § 4001(a) stating “[n]o citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress.”¹⁵³ The Supreme Court held that the government was holding Hamdi “pursuant to an Act of Congress” because the AUMF authorized the detention of enemy combatants so long as U.S. troops remain fighting in Afghanistan.¹⁵⁴ The Court concluded that detaining enemy combatants was “so fundamental and ac-

274-75 (1990).

142. Jordan, *supra* note 21, at 7.

143. *Id.*

144. Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

145. U.S. DEP’T OF JUST., LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), available at <http://news.findlaw.com/hdocs/docs/nsa/dojnsa11906wp.pdf> [hereinafter LEGAL AUTHORITIES].

146. 50 U.S.C. § 1809(a) (2000).

147. LEGAL AUTHORITIES, *supra* note 145.

148. 542 U.S. 507, 518-19 (2004).

149. *Id.* at 510.

150. *Id.*

151. *Id.* at 513.

152. *Id.* at 511.

153. *Id.* at 517.

154. *Id.* at 518-19.

cepted an incident to war as to be an exercise of the ‘necessary and appropriate force’” that Congress intended to confer upon the President.¹⁵⁵ The Bush Administration claims that similar to detaining enemy combatants, the TSP is an incident of war that is within the authority granted to the President by the AUMF.¹⁵⁶

4. *Hamdan v. Rumsfeld*

Not long after *Hamdi*, the Supreme Court altered course in its interpretation of the AUMF in *Hamdan v. Rumsfeld*. Salim Ahmed Hamdan is a Yemeni national held at Guantanamo Bay, Cuba.¹⁵⁷ Militia forces in Afghanistan provided Hamdan to the U.S. in November of 2001.¹⁵⁸ The military commission authorized to prosecute Hamdan originated from a November 13, 2001 military order signed by the President just a few weeks after the enactment of the AUMF.¹⁵⁹ This order declared that non-citizens reasonably believed to belong to al Qaeda or otherwise engaged in terrorist activities shall be “tried by military commission for any and all offenses triable by military commission.”¹⁶⁰

Pending charges by the military commission, the government appointed Hamdan a military attorney.¹⁶¹ Though Hamdan was eligible for trial by the military commission, in July 2003, no charges were filed against him until his military attorney demanded a writ of habeas corpus in the United States District Court for the Western District of Washington.¹⁶² After the habeas petition, the government charged Hamdan in 2004 with conspiracy “to commit . . . offenses triable by military commission.”¹⁶³ The district court in Washington then transferred Hamdan’s case to the United States District Court for the District of Columbia.¹⁶⁴ That court granted Hamdan’s petition on the theory that executive power to conduct military commissions is limited to offenses triable “under the law of war,” specifically the Uniform Code of Military Justice (UCMJ) and Article III of the Third Geneva Convention (Geneva Convention).¹⁶⁵ The Court of Appeals for the District of Columbia Circuit reversed the district court reasoning that Hamdan’s trial was consistent with both the UCMJ and the Geneva Convention.¹⁶⁶ The

155. *Id.* at 518.

156. Wong, *supra* note 85, at 521.

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

158. *Id.*

159. *Id.* at 2760; see Exec. Order, 66 Fed Reg. 57,833 (Nov. 13, 2001).

160. *Hamdan*, 126 S. Ct. at 2760; see Exec. Order, *supra* note 159.

161. *Hamdan*, 126 S. Ct. at 2760.

162. *Id.* at 2759-60.

163. *Id.* at 2759.

164. *Id.* at 2760.

165. *Id.* at 2761; Uniform Code of Military Justice, 10 U.S.C. §§ 801-946 (2000 & Supp. III 2005).

166. *Hamdan*, 126 S. Ct. at 2761.

Supreme Court granted certiorari on November 7, 2005.¹⁶⁷

The *Hamdan* Court carefully ruled that the military commissions exceeded the authority granted by Congress to conduct military commissions without addressing whether the commissions were within the sole constitutional authority of the President.¹⁶⁸ The Court explained that the executive's authority to run military commissions consists of authority found in the Constitution and authority granted to the executive by another branch.¹⁶⁹ The Supreme Court decided *Hamdan* on the later and left the former unaddressed.

The Constitution expressly states that Congress, not the President, possesses the power to "make Rules concerning Captures on Land and Water."¹⁷⁰ Pursuant to this authority, Congress has enacted Article 21 of the UCMJ granting the President power to conduct military tribunals but only for offenses that Congress deems may be tried in a military tribunal by statute or by the law of war.¹⁷¹ Although the Constitution's text reserves this authority for Congress, precedent suggests that the President also possesses this authority in "cases of a controlling necessity."¹⁷²

Instead of deciding if the commissions fall within the President's constitutional authority, the Court held that the military commissions exceeded the authority Congress granted the President under the UCMJ.¹⁷³ Further, the Court refused to find that the AUMF expanded the President's authorization to conduct military commissions under the UCMJ.¹⁷⁴ This narrow reading of the AUMF conflicts with the *Hamdi* decision, which held that the detention of enemy combatants was within the scope of the AUMF because it was such a fundamental incident of war.¹⁷⁵

167. *Id.*

168. *Id.* at 2759, 2773-74 (stating "[w]hether Chief Justice Chase was correct in suggesting that the President may constitutionally convene military commissions 'without the sanction of Congress' in cases of 'controlling necessity' is a question this Court has not answered definitively, and need not answer today").

169. *Id.* at 2772.

170. U.S. CONST. art. I, § 8, cl. 11.

171. Uniform Code of Military Justice, art. 21, Pub. L. 81-506, 64 Stat. 107 (codified at 10 U.S.C. § 801 (2000 & Supp. III 2005)).

172. *Ex parte* Milligan, 71 U.S. 2, 139-40 (1866) (stating it is the President who must execute the laws and within that constitutional authority he may conduct military tribunals without the consent of Congress only in emergencies).

173. *Hamdan*, 126 S. Ct. at 2759.

174. *Id.* at 2774-75.

175. *See Hamdi v. Rumsfeld*, 542 U.S. 507, 518 (2004).

IV. COMMENTARY

A. *Interpreting the TSP on Statutory Grounds, as in Hamdan, Will Raise Separation of Powers Concerns*

The *Hamdan* decision sheds light on the TSP debate because both involve Congress authorizing conduct that is arguably within the President's constitutional authority.¹⁷⁶ *Hamdan* problematically condoned congressional regulation of the President's constitutional authority to conduct military commissions.¹⁷⁷ Such an analysis is inconsistent with the separation of powers doctrine.¹⁷⁸

The Constitution provides for a government where powers are separated among the executive, legislative, and judicial branches.¹⁷⁹ James Madison wrote in *The Federalist No. 47* that concentrated accumulation of powers would result in tyranny.¹⁸⁰ Though government powers are separate, they are not static.¹⁸¹ In *Youngstown Sheet & Tube Co. v. Sawyer*,¹⁸² Justice Jackson wrote in his concurring opinion that the powers of the President fluctuate based on the actions of Congress.¹⁸³ When the President acts with express or implied authorization from Congress, his power is at a maximum because he acts with all of his constitutional power and whatever power Congress has authorized.¹⁸⁴ When the President acts without congressional authorization, his power is limited to whatever power the executive branch derives from the Constitution.¹⁸⁵ When the President acts against the will of Congress, he possesses the least power because he is limited to the sum of his own constitutional power less congressional power over the matter.¹⁸⁶

In *ACLU v. NSA*,¹⁸⁷ the District Court for the Eastern District of Michigan misapplied the separation of powers doctrine by concluding that warrantless executive surveillance violated the Constitution. The

176. Andrew C. McCarthy, *Dead Man Walking: Hamdan Sounds the Death Knell for the NSA's Terrorist Surveillance Program*, NAT'L REV. ONLINE, July 11, 2006, <http://article.nationalreview.com/?q=YTIjNWU3ZTRmYTY5YzNIOTUyM2M2Yjc4OTZkMmY2MTI=> (comparing the facts in *Hamdan* to the TSP).

177. *Hamdan*, 126 S. Ct. 2759-60.

178. McCarthy, *supra* note 176 (criticizing language in *Hamdan* suggesting that inherent presidential authority may be limited by Congress); see also LEGAL AUTHORITIES, *supra* note 145, at 28-36 (asserting that congressional regulation of inherent presidential authority violates the separation of powers doctrine).

179. See generally U.S. CONST. art. I-III (separating governmental powers).

180. THE FEDERALIST NO. 47 (James Madison), reprinted in 1 FEDERALIST AND OTHER CONSTITUTIONAL PAPERS 266 (E. H. Scott ed., 1894).

181. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring).

182. 343 U.S. 579 (1952).

183. *Id.* at 635 (Jackson, J. concurring).

184. *Id.* at 635-37.

185. *Id.* at 637.

186. *Id.* at 637-38.

187. 438 F. Supp. 2d 754 (E.D. Mich. 2006).

court ruled that Congress limited electronic surveillance to the means covered by FISA and Title III and did not grant authority to deviate from those statutes under the AUMF.¹⁸⁸ Applying the rule from Justice Jackson's concurrence in *Youngstown*, the court concluded that it should not uphold the President's act because his authority to act was at its lowest, and therefore violated the separation of powers doctrine.¹⁸⁹ The court misapplied the doctrine under the faulty assumption that the executive branch has no constitutional authority to conduct surveillance, but rather it is dependent on Congress's authority. This contradicts *Keith*, which recognized constitutional authority for executive surveillance.¹⁹⁰

Proponents of the Bush Administration contend that allowing Congress to dictate the limits of the TSP violates the separation of powers doctrine. The Administration claims the TSP is a valid exercise of the executive's inherent authority to regulate foreign affairs under Article II.¹⁹¹ The Administration contends that because the TSP is a valid exercise of constitutional authority, the President's right to conduct the TSP trumps any limitations of the FISA statute.¹⁹²

Originalists argue that permitting FISA to occupy the executive's authority to obtain foreign intelligence violates the separation of powers doctrine.¹⁹³ The Framers of the Constitution did not intend for the executive's power to protect national security to be limited by legislative authorization.¹⁹⁴ The Framers anticipated that at times national defense needed to be unburdened by checks and balances in order to defend against the speed of agile foreign enemies.¹⁹⁵

The Framers' logic is reflected in modern public policy arguments suggesting that some of the FISA limitations are too outdated to combat terrorism. Simply put, requiring compliance with FISA hinders the government's ability to move as quickly as the terrorists. FISA critics argue that the time-consuming procedural hurdles of obtaining a FISA warrant were appropriate when the Act passed in 1978, but are too obsolete to allow the government to track intelligence at the speed which data now moves thirty years later.¹⁹⁶ Proponents of the TSP claim the time required to prepare legal briefs and obtain judicial approval will slow the government's response in situations where less than twenty-four

188. *Id.* at 779.

189. *ACLU*, 438 F. Supp. 2d at 778.

190. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 310 (1972).

191. LEGAL AUTHORITIES, *supra* note 145.

192. *Id.*

193. McCarthy, *supra* note 176.

194. *Id.*

195. *Id.* (stating that the Framers envisioned the need for a flexible executive branch even before "weapons of mass destruction coexisted with communications systems that can transmit orders from Kandahar to New York in the click of a mouse").

196. Press Release, *supra* note 58, at 3.

hours can mean the difference between thwarting, or experiencing a terrorist attack.¹⁹⁷

B. Interpreting the AUMF to Determine Presidential Authority for Conducting the TSP Will Contradict Precedent

The *Hamdan* decision has left the Supreme Court in a position where it cannot address the statutory authority for the TSP without contradicting precedent.¹⁹⁸ The Bush Administration offers that the AUMF, FISA, and Title III form consistent links in a chain authorizing the TSP.¹⁹⁹ Title III allows electronic surveillance as permitted by FISA. FISA then allows surveillance as authorized by Congress. Congress in turn authorized surveillance under the AUMF.²⁰⁰ The Bush Administration claims that in enacting the AUMF, Congress vested the President with the power to act as necessary to prevent further terrorist attacks.²⁰¹ The Bush Administration reinforces this argument with the language from *Hamdi* stating that the AUMF grants the President authority to use force that includes the “fundamental incident[s] of waging war.”²⁰² The President views the TSP as a fundamental incident of the war on terror.²⁰³ The government views the AUMF as a specific statutory grant from Congress to deviate from FISA when necessary to protect national security.²⁰⁴

The *Hamdan* Court’s interpretation of the AUMF is problematic to the Bush Administration’s theory. In *Hamdan*, the government argued that the AUMF specifically authorized the type of military commission used to try Hamdan.²⁰⁵ The Supreme Court, however, found this unconvincing and refused to accept that Congress intended the broad language of the AUMF to expand presidential authority beyond the UCMJ statutes.²⁰⁶

This idea reappeared in *ACLU v. NSA*. There, the government asserted the same argument from *Hamdan*—that the AUMF authorized deviation from the UCMJ but this time with respect to FISA.²⁰⁷ Like in *Hamdan*, this argument failed.²⁰⁸ The *ACLU* court reasoned that the AUMF is silent about intelligence or surveillance.²⁰⁹ The court ruled

197. *Id.*

198. See McCarthy, *supra* note 176.

199. LEGAL AUTHORITIES, *supra* note 145, at 3.

200. *Id.* at 2; see Wong, *supra* note 85, at 521.

201. LEGAL AUTHORITIES, *supra* note 145, at 2.

202. Gonzalez, *supra* note 56.

203. See LEGAL AUTHORITIES, *supra* note 145, at 11.

204. Gonzalez, *supra* note 56.

205. Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2775 (2006).

206. *Id.* (stating “there is nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth in *Article 21 of the UCMJ*”).

207. *ACLU v. NSA*, 438 F. Supp. 2d 754, 779 (E.D. Mich. 2006).

208. *Id.*

209. *Id.*

that authorization to deviate from FISA could not be implied, rather, Congress intended Title III and FISA to be the exhaustive means for conducting electronic surveillance.²¹⁰

The *ACLU* court justified this conclusion with an exercise in statutory construction.²¹¹ FISA is specific and the AUMF is general. When analyzing conflicting interpretations, specific provisions govern general provisions.²¹² The court found relevant language in *Hamdi* from Justice O'Connor explaining that authorization under the AUMF has limits.²¹³ O'Connor wrote that the AUMF authorized the detention of an enemy combatant because it was a fundamental incident of war; however, the Fifth Amendment limits the AUMF.²¹⁴ The *ACLU* court applied this same framework. Authority under the AUMF is limited by the Constitution, and the court found the TSP violated the Fourth Amendment. The court's decision to interpret the AUMF narrowly is difficult to reconcile with the broad interpretation from *Hamdi*.

C. The Modern Media Has Rendered the State Secrets Doctrine into an Ineffective Analysis Tool

The previously mentioned *Hepting v. AT&T Corp.* decision demonstrates how the modern media's intense exposure limits the application of the state secrets doctrine rendering it an outdated form of analysis. In *Hepting*, the plaintiffs sought to discover details regarding government surveillance at a San Francisco AT&T office.²¹⁵ The government sought dismissal under the state secrets doctrine.²¹⁶

The *Hepting* court initially determined whether the information asserted was actually a secret for purposes of the privilege.²¹⁷ The court did not agree with the government that confirming or denying the truth of information already publicly leaked to the media aids terrorists.²¹⁸ The court distinguished this case from previously dismissed cases because revealing the subject matter would threaten national security.²¹⁹ The court stated that none of the previous cases involved such widespread constitutional violations as the plaintiffs alleged.²²⁰ According to the court, one of the previous cases, *El-Masri v. Tenet*,²²¹ was distinguishable because it involved a secret program that was relatively un-

210. *Id.*

211. *Id.*

212. *Id.* (quoting *Morales v. TWA, Inc.*, 504 U.S. 374 (1992)).

213. *Id.* at 779-80.

214. *Id.*

215. *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 979 (N.D. Cal. 2006).

216. *Id.* at 985.

217. *Id.* at 986-89.

218. *Id.* at 989-90.

219. *Id.* at 994.

220. *Id.*

221. 437 F. Supp. 2d 530 (E.D. Va. 2006).

known, whereas here, the program was well-publicized by the media.²²² The court used the media coverage to justify permitting discovery.²²³ The media ultimately usurped the protections of the state secrets doctrine. The court granted the plaintiffs limited discovery, but reserved the possibility that after further discovery the privilege may preclude certain evidence and entitle AT&T to summary judgment.²²⁴ In the court's words, "dismissing this case at the outset would sacrifice liberty for no apparent enhancement of security."²²⁵

Media coverage also marginalized the state secrets doctrine in *ACLU v. NSA*. There, the plaintiffs contended that the TSP and other data-mining programs impaired their right to communicate with people in the Middle East and violated the Constitution.²²⁶ The court found that the plaintiffs could prove their case entirely with statements reported in the media and thus denied in part the government's request for dismissal pursuant to the state secrets doctrine.²²⁷

V. THE SPECIAL NEEDS EXCEPTION AND STATISTICAL SCIENCE AS A LESS PROBLEMATIC ALTERNATIVE APPROACH

The Bush Administration insists that the FISA limitations are outdated.²²⁸ Critics allege that unchecked, warrantless surveillance violates FISA and the Constitution.²²⁹ As discussed in Part IV, neither side has produced an argument that is consistent with the separation of powers doctrine and precedent. The state secrets doctrine no longer provides useful analysis because modern media practices have rendered it obsolete. It is time for a new approach. An alternative analysis is to frame warrantless executive surveillance in terms of the special needs exception to the Fourth Amendment and then use statistical forecasting to measure the extent of the special need.

As discussed in Part III, special needs of law enforcement sometimes permit suspicionless exceptions to the Fourth Amendment.²³⁰ Warrantless executive surveillance of foreign intelligence threats is

222. *Hepting*, 439 F. Supp. 2d at 994.

223. *Id.* The court also refused to dismiss the case under either of two statutory privileges claimed by the government. *Id.* at 994-95. 50 U.S.C. § 403-1(i)(1) (2006) states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." *Id.* at 998. 50 U.S.C. § 402 (2006) states that

[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

Id.

224. *Id.* at 994-95.

225. *Id.* at 995.

226. *ACLU v. NSA*, 438 F. Supp. 2d 754, 758 (E.D. Mich. 2006).

227. *Id.* at 764-66.

228. Press Release, *supra* note 58, at 3.

229. See Risen & Lichtblau, *supra* note 12.

230. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000).

probably within the special needs exception to the Fourth Amendment.²³¹ Once viewed in this light, statistics may indicate whether a specific timeframe for surveillance is sufficient in duration to address the special needs of law enforcement. To explore this question, courts should instruct the government to compile statistical data that addresses how many days of surveillance are necessary to determine the existence or absence of probable cause. Probability forecasts based on past data may prove that after several days without success, the likelihood of continued surveillance generating probable cause becomes too remote to justify a special needs exception to the Fourth Amendment. A past government study has already demonstrated the ability to forecast the intensity of future threats with statistical science in other areas of criminal law.²³²

Government collection of statistical data is common. In fact, the DOJ already has a data-collection department in place, which could produce statistical data on wiretapping. The DOJ maintains a vast collection of crime related statistics through the Bureau of Justice Statistics (BJS).²³³ The Justice Systems Improvement Act of 1979 established the BJS on December 27, 1979.²³⁴ Annually, BJS interviews over 70,000 citizens to record the circumstances of criminal activity.²³⁵ The BJS organizes this data into periodic reports and shares it with policymakers over the internet.²³⁶

A 1997 report, entitled *Lifetime Likelihood of Going to State or Federal Prison*, demonstrates the BJS's data-collection capability.²³⁷ In this special report, the BJS statisticians collected the first-time incarceration ages of a large sample of people and organized the data by race and gender.²³⁸ Based on this data, the BJS forecasted that a newborn American has a 5.1% chance of going to prison at some point in their lifetime.²³⁹ The BJS also concluded that the likelihood of an individual going to prison during their lifetime decreases with age.²⁴⁰ Accordingly, the probability of an individual going to prison for the first time after age forty-five is less than one percent.²⁴¹

The relevant data for an analysis of the TSP would necessitate a large sample of past warrantless surveillance missions, all of which even-

231. *See id.* at 44.

232. *See* BUREAU OF JUST. STAT., U.S. DEP'T OF JUST., *LIFETIME LIKELIHOOD OF GOING TO STATE OR FEDERAL PRISON* 3 (1997).

233. *See* About the Bureau of Justice Statistics, <http://www.ojp.usdoj.gov/bjs/aboutbjs.htm> (last visited Sept. 27, 2007).

234. *Id.*

235. *Id.*

236. *Id.*

237. BUREAU OF JUST. STAT., *supra* note 232, at 2-3.

238. *Id.* at 10.

239. *Id.* at 3.

240. *Id.*

241. *Id.*

tually resulted in a finding of probable cause. In the incarceration study, data collectors measured the number of years transpiring before an individual first entered prison.²⁴² With respect to wire-tapping, data-collectors could group each surveillance mission by the number of days of surveillance transpiring before capturing evidence sufficient to support probable cause. The number of days transpiring before the finding of probable cause for each particular mission would serve as random variables, which can yield statistical relationships.

A statistics-based study may yield the potential to forecast the duration of surveillance needed to uncover evidence of probable cause in the same way the incarceration study forecasted duration until incarceration. Statistics could prove that continuing surveillance after a given number of unsuccessful days of surveillance yields too little benefit to justify continued wire-tapping. The chances of one becoming first incarcerated between the age of sixty-five and death is statistically very low; similarly, the chance of developing probable cause after a given duration of unsuccessful surveillance may also prove to be too remote to justify a special needs exception to the warrant requirement.

VI. CONCLUSION

Advances in technology have made electronic surveillance more effective and more intrusive at the same time. Although technology evolves daily, until recently, FISA has remained dormant and unchanged for nearly thirty years. While Congress works to amend the FISA framework, current and future administrations will undoubtedly continue to engage in electronic surveillance for the sake of national security. In drafting a new FISA, policymakers should create an avenue for statutory surveillance that is adequate to protect national security but does not allow monitoring of threats too remote to be outside the special needs exception to the Fourth Amendment. The new FISA could achieve this by imposing a data-keeping requirement on the government. Analyzing statistical data with respect to past surveillance conducted may offer a means for using past performance to gauge the severity of future threats. Probability forecasts could prove that after a given time period without success, the probability of continued surveillance resulting in probable cause becomes too faint to justify a special needs exception to the Fourth Amendment.

242. BUREAU OF JUST. STAT., *supra* note 232, at 2.