

WHO KNOWS YOU ARE READING THIS? UNITED STATES' DOMESTIC ELECTRONIC SURVEILLANCE IN A POST- 9/11 WORLD

*Kenneth R. Logsdon**

I. INTRODUCTION

If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.¹

Two essential provisions within the Constitution of the United States of America that attempt to distinguish between governmental prerogative and individual liberty are the First and Fourth Amendments.² Accordingly, the Constitution and subsequent Supreme Court prescriptions have created rights in which an American citizen's privacy and speech must be respected by state and federal governmental officials.³

Nevertheless, since the Civil War, the United States Government has continually infringed upon those rights via electronic monitoring programs directed towards the general public.⁴ Incongruously, this monitoring has continued subsequent relatively recent dictates by the Supreme Court that the United States Government must respect one's right to privacy.⁵ Additionally, this monitoring activity has accelerated since the terrorist attacks of September 11, 2001 ("9/11").⁶

This Note will explore the United States Government's electronic

* J.D., University of Illinois College of Law, 2009; B.S., Criminal Justice, Utah Valley State University, 2005.

1. THE FEDERALIST NO. 51 (James Madison).

2. See *infra* Parts II, III.

3. See *infra* Part II.A.

4. See *infra* Part II.A.

5. See *infra* Part II.A.

6. See *infra* Part II.B.

surveillance of American citizens in a post-9/11 world and the constitutional implications of such action. Part II will explain the history and developments of electronic surveillance in the United States from the Civil War to present. Part III will discuss and analyze the latest developments and implications of electronic surveillance in relation to the First Amendment, Fourth Amendment, and the constitutional doctrine of separation of powers. Part IV will discuss and recommend a modified application of the National Security Letters Reform Act of 2007, Congress's latest attempt to narrow the scope of the Executive Branch's electronic surveillance capabilities. Finally, Part V will summarize and conclude this Note.

II. BACKGROUND

The United States Government was created to "form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty"⁷ The Fourth Amendment to the United States Constitution 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 particularly describing the place to be searched, and the persons or things to be seized.⁸

The Fourth Amendment was a radical concept and the rights within had never been recognized by any government prior to the ratification of the Constitution.⁹

Nonetheless, the practice of domestic electronic surveillance within the United States is extensive and has existed as early as the Civil War.¹⁰ In light of this history, the United States Supreme Court and Congress have attempted to define the government's electronic monitoring prerogatives while respecting individual constitutional rights.¹¹ This treacherous and intricate Congressional undertaking has become appreciably more complicated since the 9/11 terrorist attacks,¹² due in large part to the Executive Branch's insistence that more flexible standards of electronic surveillance are necessary to protect America from another attack.¹³

7. U.S. CONST. pmbl.

8. U.S. CONST. amend. IV.

9. Judge Andrew Napolitano, Address at the Reason Magazine Conference, Washington D.C.: Civil Liberties During Wartime (Oct. 26, 2007), available at http://www.fff.org/classroom/2007_pdf/2007_Napolitano.pdf.

10. *An Examination of the Call to Censure the President: Before the S. Comm. on the Judiciary*, 109th Cong. (2006) (statement of Robert F. Turner, Associate Director, Center for National Security Law, University of Virginia) (stating President Abraham Lincoln authorized the tapping of telegraph lines during the Civil War).

11. *Id.*

12. See *infra* Part II.B (explaining electronic surveillance in the United States post-9/11).

13. See *infra* Part II.B.

*A. Electronic Surveillance in the United States Pre-9/11*¹⁴

One year before the bombing of Pearl Harbor, President Franklin D. Roosevelt authorized the FBI to intercept any communications, either domestic or abroad, of persons suspected of engaging in subversive actions against the United States.¹⁵ He did so even though the Supreme Court had already stated that such conduct, without a warrant, was unconstitutional.¹⁶

In 1967, the Supreme Court determined that an individual had a reasonable expectation of privacy, absent probable cause, in the content of their telephone conversations, even while in a public place.¹⁷ This right to privacy also applied to threats of domestic acts of terrorism.¹⁸ However, in 1979 the Supreme Court did not find this privacy extended to one's telephone records because one does not have a reasonable expectation of privacy in information readily available to a third party.¹⁹ Accordingly, one "assumes the risk" that the telephone numbers called and received on their subscriber line will be used by private businesses and police.²⁰

1. Omnibus Crime Control and Safe Streets and Electronic Communications Privacy Acts

The standards articulated by the Supreme Court regarding electronic surveillance in regular criminal investigations are codified in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")²¹ and the Electronic Communications Privacy Act of 1986 ("ECPA").²² The creation of the ECPA was necessary because "two established lines of Fourth Amendment doctrine . . . strongly suggested that if the Constitution was the sole source of protection for remotely-stored electronic communications, then third parties, including the government, would face no obstacle to compelling disclosure."²³ Accordingly, the ECPA embodies Congress's belief that new federal statutes

14. "9/11" is a reference to the events that occurred on September 11, 2001, when "the al Qaeda terrorist network used hijacked commercial airliners to attack prominent targets in the United States. Approximately 3,000 people were killed in those attacks." *Hamdi v. Rumsfeld*, 542 U.S. 507, 510 (2004).

15. John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 588 (2007).

16. *See Nardone v. United States*, 302 U.S. 379, 379 (1937) (determining that the Federal Communications Act of 1934 prohibits the interception of telephone calls absent a warrant).

17. *Katz v. United States*, 389 U.S. 347, 351–52 (1967).

18. *See United States v. U.S. Dist. Court*, 407 U.S. 297, 342 (1972) (weighing the Attorney General's opinion that a wiretap was necessary against the right to privacy).

19. *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

20. *Id.* at 744.

21. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510–20 (2000 & Supp. 2003)).

22. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2232, 2510–21, 2701–11, 3117, 3121–26 (2000 & Supp. 2003)). *See generally* U.S. Internet Serv. Provider Ass'n, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945 (2003) (providing "general guidelines for Internet service provider compliance with law enforcement and national security evidence gathering authorities.").

23. Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 574 (2007).

were necessary to ensure that privacy interests in new forms of electronic communication were protected by well established constitutional standards.²⁴ Thus, the ECPA expounded upon Title III's ability to monitor oral communications to also include data in digital form.²⁵

The ECPA is applied to "electronic communication" or "remote computing" services.²⁶ To illustrate, an Internet service provider ("ISP"):

may qualify as either a provider of "electronic communication service" or "remote computing service" – or both. Take, for example, the case of a single e-mail received by an ISP for one of its customers. Before the recipient opens the e-mail, the ISP is providing "electronic communication service" because it is providing the user "the ability to . . . receive . . . electronic communications." Once the e-mail has been opened, however, the electronic communication is complete. If the user does not immediately delete the e-mail, the ISP is now offering a "remote computer service." It is providing "computer storage" of the opened e-mail for the user.²⁷

Interestingly, messages that are posted to group message boards present a distinctive problem. "It is [very] difficult, if not impossible to determine if all members of a group [messaging board] have read the message."²⁸ Accordingly, for some members, the hosting server of the messaging board "is merely providing storage while for others[, it] is still in the process of delivering the message. How to treat such group message boards thus presents difficult legal and technical questions."²⁹

Congress defined the term "electronic communication" broadly in order to encompass a wide range of technologies including "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . ."³⁰ Aside from customer consent, a public service provider may only disclose customer records to the government in response to a subpoena or court order.³¹ The types of customer information the government can receive via a subpoena is limited to Internet Protocol address information and billing information if the service provider is charging the subscriber for services.³²

All other noncontent customer records such as transactions, Web site visitations, and e-mail correspondence, can only be obtained by the government with a court order or search warrant.³³ Additionally, the government may install either a pen register (a device that records the

24. *Id.* at 573.

25. 18 U.S.C. §§ 2510(12), (15) (2000).

26. *Id.* § 2711(2) (2000 & Supp. 2003).

27. U.S. Internet Serv. Provider Ass'n, *supra* note 22, at 950 (citing 18 U.S.C. § 2510(15)).

28. *Id.* at n.12.

29. *Id.*

30. 18 U.S.C. § 2510(12).

31. *Id.* § 2703.

32. *Id.* § 2703(c)(2).

33. *Id.* § 2703(d).

telephone numbers dialed on outgoing calls) or a trap and trace device (a device that records the originating numbers of incoming calls) with a court order.³⁴ Pen register and trap and trace devices are not solely limited to telephone numbers, and may include routing and addressing information.³⁵ In emergency situations (such as imminent death or bodily injury or threats to national security), law enforcement may implement a pen register or trap and trace device without a court order, so long as an order is obtained within forty-eight hours.³⁶ Although service providers are required by law to cooperate, law enforcement is also obligated to compensate the provider for all reasonable expenses.³⁷

Further, the ECPA allows for governmental access to the contents of electronic communications *not* in electronic storage or data older than 180 days, via subpoena or court order.³⁸ The data not in “electronic storage” includes “photos, address books, calendars, web sites, files, documents, and other types of content” stored on the ISP’s server(s).³⁹ This is significant because the simple requirement of a subpoena, as opposed to a warrant, is all that is needed to acquire basic user account information on any particular subscriber.⁴⁰

Nonetheless, “electronic storage” is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection . . .”⁴¹ This has been read to apply to cases in which a user sends a message to another user and the message resides on the recipient server, but the receiver has yet to read or download the message.⁴² Recent rulings have expanded this definition to include messages that have been read and remain stored on the ISP’s server(s).⁴³

If the information in electronic storage is older than 180 days and the government is using a subpoena or court order, rather than a warrant, notice must be given to the customer.⁴⁴ However, if law enforcement believes notice would “[s]eriously jeopardiz[e] an investigation,” notice can be delayed ninety days.⁴⁵ To acquire information found within electronic storage for 180 days or less, the government must acquire a warrant.⁴⁶ Following the latest developments determining that “electronic storage” also includes opened e-mail, most major ISPs require a search warrant before divulging any e-mail

34. *Id.* § 3121(a).

35. *Id.* § 3127(3).

36. *Id.* § 3125(a).

37. *Id.* § 3124(a)–(c).

38. *Id.* § 2703(a)–(b).

39. Zwillinger & Genetski, *supra* note 23, at 581.

40. 18 U.S.C. § 2703(d).

41. *Id.* § 2510(17).

42. *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461–62 (5th Cir. 1994).

43. Zwillinger & Genetski, *supra* note 23, at 579–80.

44. 18 U.S.C. § 2703(a)–(b).

45. *Id.* § 2705(a).

46. *Id.* § 2703(a).

message less than 180 days old.⁴⁷

There are different rules applied to the interception of electronic information. An “intercept” is defined as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”⁴⁸ In order to intercept electronic information the government must obtain a court order, and the duration is limited to 30 days.⁴⁹

Significantly, the ECPA also allowed for the Federal Bureau of Investigation (“FBI”) to compel electronic service providers to produce customer billing and transactional records so long as the FBI could show that the records pertained to a foreign counterintelligence investigation and that specific and articulable facts were present to link the suspect to a foreign power.⁵⁰ The self-certification procedure pursuant to this provision became known as National Security Requests⁵¹ communicated via a National Security Letter (“NSL”).⁵²

Further, the government could obtain a court order prohibiting the electronic communications provider from disclosing the inquiry to the subscriber in question.⁵³ In 1994, this provision was relaxed to allow self-certification by an FBI agent so long as the subscriber had contact with an intelligence officer or suspected terrorist.⁵⁴ As a result, the subscriber no longer needed to actually be an agent of a foreign power.⁵⁵

2. *The Privacy Act of 1974*

The United States Government’s ability to gather and mine data on its citizens is tempered by The Privacy Act of 1974.⁵⁶ The Act is applicable to many different forms of data and regulates the government’s collection, storage, use, transfer, and modification of data.⁵⁷ The Act imposes several duties on governmental agencies. To begin with, if an agency chooses to acquire and use a database of information about citizens, it must make this

47. Zwillinger & Genetski, *supra* note 23, at 581.

48. 18 U.S.C. § 2510(4).

49. *See id.* §§ 2516, 2518 (detailing requirements for authorization and procedure for obtaining court order to intercept).

50. *Id.* § 2709; *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 481 (S.D.N.Y. 2004).

51. *See Doe v. Gonzales*, 500 F. Supp. 2d 379, 390 (S.D.N.Y. 2007) (distinguishing national security requests from letters in that request pertains to a certain individual while a letter may contain multiple requests). An example of a letter with multiple requests can be found at http://www.aclu.org/safefree/nationalsecurityletters/released/dod_100207release_1_48.pdf.

52. *Ashcroft*, 334 F. Supp. 2d at 480. In addition, “[s]ection 2709 is one of only a handful of statutes authorizing the Government to issue NSLs. The other NSL statutes authorize the Government to compel disclosure of certain financial and credit records which it certifies are relevant to international terrorism or counterintelligence investigations, and to compel disclosure of certain records of current or former government employees who have (or have had) access to classified information.” *Id.*; *see also* 12 U.S.C. § 3414 (2000) (financial records); 15 U.S.C. § 1681u (2000) (credit records); 50 U.S.C. § 436 (2000) (requests by authorized investigative agencies).

53. 18 U.S.C. § 2705(b) (2000).

54. 18 U.S.C. § 2709 (1994); *Ashcroft*, 334 F. Supp. 2d at 481.

55. *Ashcroft*, 334 F. Supp. 2d at 481.

56. 5 U.S.C. § 552a (2000).

57. *Id.* § 552a(a).

publicly known via a notice in the Federal Register.⁵⁸ The data gathered can only be for the purpose of the agency as set forth by statute or executive order.⁵⁹ Any information obtained cannot be shared with another agency without the affected individuals' consent.⁶⁰ Further, individuals have the right to obtain their recorded information to make sure it is correct.⁶¹

Notwithstanding the many procedural safeguards contained within the Act, there are many exemptions at the government's disposal, and enforcement mechanisms are generally ineffective. For instance, the primary enforcement mechanism is the imposition of civil damages in a federal court; however, individuals have a difficult time establishing rectifiable injuries.⁶² Regarding exemptions, an agency is not obligated to disclose it is sharing information with another agency if the public is notified in the creation of the system that the disclosure is routine or compatible with the purpose for which the information was originally collected.⁶³

Nevertheless, an agency can even dispense with the initial notice of inter-agency information sharing if the transfer is for law enforcement purposes and requested by the receiving agency's head.⁶⁴ Further, a law enforcement agency, such as the Central Intelligence Agency ("CIA"), may be exempt from most provisions (general exemptions) of the act if the agency head publishes a notice to that effect,⁶⁵ and any agency may be exempt from some of the provisions (specific exemptions) if notice is given that it is for national defense or foreign policy.⁶⁶ Interestingly, general exemptions are not applicable to the National Security Agency ("NSA").⁶⁷ This may be insignificant; however, the NSA uses the Federal Register to give notice of specific exemptions and invokes the law enforcement privilege exemption when needed.⁶⁸

3. Foreign Intelligence Surveillance Act

In conjunction with the aforementioned constitutional and statutory restrictions applied to electronic surveillance of American citizens, Congress devised a new mechanism for surveillance of noncitizens via the Foreign Intelligence Surveillance Act of 1978 ("FISA").⁶⁹ FISA began, not as a

58. *Id.* § 552a(e)(4).

59. *Id.* § 552a(e)(1).

60. *Id.* § 552a(b)(d).

61. *Id.*

62. *Id.* § 552a(g); see also Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV 609, 633 (2007) ("[W]hat court would award damages because a government agency asked too many questions, and too many irrelevant questions?").

63. 5 U.S.C. § 552a.

64. *Id.* § 552a(b)(7).

65. *Id.* § 552a(j).

66. *Id.* § 552a(k).

67. *Id.* § 552a(j) (stating general exemptions apply to the CIA or any agency "which performs as its principal function any activity pertaining to the enforcement of criminal laws . . .").

68. Bignami, *supra* note 62, at 634.

69. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801, et seq. (2002)). See generally Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147 (2006) (criticizing the Bush administration's warrantless monitoring of citizens

separate act, but as an amendment to the aforementioned Title III.⁷⁰ Congress's goal was to "provide the secure framework by which the executive branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights."⁷¹ In the process, Congress created a new specialized court, the Foreign Intelligence Surveillance Court ("FISC"), to hear and either grant or deny requests to electronically surveil individuals so long as the purpose of the surveillance was foreign intelligence.⁷²

Congress's motivation for the creation of FISA was precipitated by the abuse of executive power by President Richard M. Nixon during the Vietnam War and lengthy abuse by the FBI.⁷³ Specifically, President Nixon was heavily concerned about domestic opposition to the Vietnam War and suspected foreign elements were instigating the opposition.⁷⁴ Accordingly, President Nixon created an intelligence gathering program known as the "Hutson Plan," which applied systematic use of wiretappings, burglaries, mail openings, and infiltration against antiwar groups and other suspect associations.⁷⁵ The plan was only in operation for five days before FBI Director J. Edgar Hoover terminated it.⁷⁶ Nixon's approval of the plan, and his explicit knowledge of its illegality, was cited in his Articles of Impeachment.⁷⁷

Though J. Edgar Hoover terminated the Hutson Plan only five days after it had been implemented, he had been overseeing an anticommunist program known as COINTELPRO from 1956 to 1971 as part of "a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence."⁷⁸ The activities engaged in under COINTELPRO between 1960 and 1974 included illegal use of over 2,300 wiretaps, 697 bugs (listening devices), and 57,000 mail openings.⁷⁹

For that reason, FISA requires probable cause that the target is a foreign agent or acting on behalf of a foreign power, in order to obtain electronic communications even in emergency situations.⁸⁰ Nonetheless, the standard of probable cause is slightly less than that in the regular criminal context because "FISA does not require a finding that a crime is imminent or that the elements

through the powers given to the NSA).

70. Bloom & Dunn, *supra* note 69, at 158.

71. S. REP. NO. 95-604, pt. 1, at 15 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916.

72. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801, et seq. (2002)).

73. Bloom & Dunn, *supra* note 69, at 149-50.

74. *Id.* at 149.

75. *Id.*

76. *Id.*

77. H.R. REP. NO. 93-1305, at 146 (1974).

78. Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1080 (2002) (citing S. REP. NO. 94-755 (1976)).

79. *Id.* at 1081.

80. 50 U.S.C. §§ 1805(a)(3), (f) (2000).

of a specific crime exist, but it requires instead a more speculative standard that allows surveillance to occur at an earlier stage in the investigative process.”⁸¹

In case of a declaration of war by Congress, FISA allows the President, through the Attorney General, a fifteen day period from the date of the declaration to perform electronic surveillance without a warrant.⁸² In nonwartime situations, a wiretap can be put in place without judicial approval, so long as approval is obtained within seventy-two hours.⁸³ In addition, the Attorney General can authorize the use of a pen register or trap and trace device without court order so long as the Attorney General believes an emergency exists that requires immediate installation and applies for a FISA Court order within forty-eight hours.⁸⁴

One notable exception to court-ordered surveillance is when the Attorney General seeks to surveil an official of a foreign power.⁸⁵ In these situations the Executive Branch can monitor a foreign official without a court order for up to one year so long as the Attorney General certifies in writing that: (1) the target is a foreign official, (2) there is no likelihood a United States citizen⁸⁶ will be a party to the communication, and (3) that minimal procedures are in place.⁸⁷ In such situations, the Attorney General can also request that the communications provider not alert the subscriber to the surveyed activity.⁸⁸ Notably, FISA contains a provision stating that any electronic surveillance performed by the government without authorization by statute constitutes a criminal offense.⁸⁹

4. *The National Security Agency*

As previously explained, the United States Government is restricted as to its ability to acquire information of an individual’s personal communication that transpires domestically or across a United States boundary.⁹⁰ That raises the question: What are the United States Government’s restrictions regarding individuals residing outside its jurisdictional boundaries? That is where the NSA comes into play.⁹¹

81. Bloom & Dunn, *supra* note 69, at 164.

82. 50 U.S.C. § 1811.

83. *Id.* § 1805(f).

84. *Id.* § 1843(a)–(b) (2000 & Supp. 2003).

85. *Id.* § 1802(a).

86. A “United States person” is defined by FISA as “a citizen of the United States, an alien lawfully admitted for permanent residence . . . an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.” *Id.* § 1801(i).

87. *Id.* § 1802(a)(1).

88. *Id.* § 1802(a)(4)(A) (directing communications providers to give the Attorney General the requested information in “a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers . . .”).

89. *Id.* § 1809(a)(1).

90. *See supra* Part II.A.(1)–(3).

91. Bloom & Dunn, *supra* note 69, at 153.

The NSA was created in 1952 by President Harry S. Truman and the National Security Council via an executive directive.⁹² The NSA is the United States' largest intelligence agency and acquires data from all forms of electronic information with listening posts throughout the world, through a program referred to as Echelon.⁹³ According to Porter Goss, former CIA Director and Chairman of the House Intelligence Committee, the NSA has the ability to monitor every phone call in the world.⁹⁴ Nevertheless, the NSA maintains that it recognizes and adheres to constitutional limitations on the United States Government's ability to monitor its citizens.⁹⁵ Further, the NSA maintains that all information gathered "is specifically limited to that on foreign powers, organizations or persons and international terrorists."⁹⁶

Though the NSA maintains that it adheres to constitutional restrictions when surveilling United States citizens, the agency's history tells a different story.⁹⁷ In fact, President Nixon's Hutson Plan was made possible by the capabilities of the NSA.⁹⁸ Specifically, the NSA created a:

"watch list" of activity whereby the NSA sorted through the electronic communication captured by identifying particular words, names, subjects, and locations . . . entail[ing] the placement of American citizens and organizations on the watch list . . . justif[ying] the activity not only based upon the national security need for the information, but also because it expanded the term "foreign intelligence" to require only one foreign terminal from which the communications originated.⁹⁹

The NSA's ability to define foreign intelligence to include domestic terminals and persons is what led to congressional criticism.¹⁰⁰ Prior to the termination of this activity in 1973, the NSA also expanded its focus to include international drug trafficking and acts of terrorism.¹⁰¹ The domestic surveillance role of the NSA has been reinstated and heightened subsequent 9/11.¹⁰²

B. Electronic Surveillance in the United States Post-9/11

The events of 9/11 prompted the United States Government to pass new

92. *Id.* at 152; National Security Agency Frequently Asked Questions, About NSA, <http://www.nsa.gov/about/about00018.cfm#3> (last visited Oct. 4, 2008).

93. *Ex-Snoop Confirms Echelon Network Global Network Monitors Phones and Email*, CBS NEWS, Mar. 1, 2000, <http://www.cbsnews.com/stories/2000/02/24/60minutes/main164651.shtml>. According to former Canadian spy Mike Frost, Echelon is used by the global intelligence community to gather any information needed, even on an agencies own government. *Id.*

94. *Id.*

95. National Security Agency, Signals Intelligence, <http://www.nsa.gov/sigint/index.cfm> (last visited Oct. 4, 2008).

96. *Id.* The NSA adheres to directives from all departments and levels of the U.S. Executive Branch. *Id.*

97. Bloom & Dunn, *supra* note 69, at 156-57.

98. *Id.* at 157.

99. *Id.*

100. *Id.*

101. *Id.*

102. *See infra* Part II.B.

aggressive anti-terror legislation that implemented new investigative procedures to accommodate advancements in technology.¹⁰³ Independently, the Executive Branch of the United States created a new surveillance program that implemented the technological capabilities of the private telecommunications industry in order to bolster the government's authorization to electronically surveil individuals as prescribed by FISA.¹⁰⁴

1. *The USA PATRIOT ACT*

The USA PATRIOT ACT ("PA") was passed shortly after the terrorist attacks of 9/11, following brief Congressional debate during a time when both Houses were out of office because of anthrax scares.¹⁰⁵ In fact, not a single representative even read the Act, or had time to read it, prior to voting.¹⁰⁶ This Act drastically changed the rules of intelligence gathering and subsequently led to the creation of the Homeland Security Department.¹⁰⁷

To begin, the PA modified FISA by requiring that intelligence gathering be merely a "significant purpose" rather than the sole "purpose" of the warrant.¹⁰⁸ The PA also amended FISA by clearly stating that the government may use pen register and trap and trace devices to capture routing information for electronic communications.¹⁰⁹ In particular, FISA's original statutory language had referred to "telephone lines," which made it uncertain whether a pen register or trap and trace device could be extended to include Internet communications. Accordingly, the PA resolved this ambiguity by expanding FISA language to include any "other facility to which the pen register or trap and trace device is to be attached or applied."¹¹⁰

The ECPA was also amended to include two new provisions.¹¹¹ First, the federal courts were given the authority to issue pen register and trap and trace orders outside the district of the issuing court.¹¹² Second, law enforcement authorities were provided the capability to install their own monitoring device to perform pen registers and trap and traces on computers belonging to the ISPs so long as they filed a special report with the court.¹¹³ Federal courts were also granted the ability to compel assistance from any ISP in the United States allowing one order to be served on multiple ISPs.¹¹⁴ Further, federal

103. See e.g., United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 218, 155 Stat. 272, 291.

104. See *infra* Part II.B.3.

105. Michael P. O'Connor & Celia M. Rumann, *Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland*, 24 CARDOZO L. REV. 1657, 1705 (2003).

106. Judge Andrew Napolitano, *supra* note 9 (stating the House had only fifteen minutes to read over the act prior to ratification).

107. O'Connor & Rumann, *supra* note 105, at 1707.

108. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

109. 50 U.S.C. § 1842(d)(2)(A) (2000).

110. *Id.*

111. U.S. Internet Serv. Provider Ass'n, *supra* note 22, at 959.

112. 18 U.S.C. § 3123 (2000).

113. *Id.*

114. *Id.*

courts were empowered to authorize the use of pen registers and trap and trace devices in other districts allowing a court in one state to compel an ISP in another to assist in an investigation under its pen register or trap and trace order.¹¹⁵

Notably, the government's use of NSLs was also greatly expanded. Specifically, the PA "removed the previous requirement that § 2709 inquiries have a nexus to a foreign power, replacing that prerequisite with a broad standard of relevance to investigations of terrorism or clandestine intelligence activities."¹¹⁶ To illustrate, before the PA, the government had:

to show specific facts that would lead the person issuing the [NSL] to conclude that the person about whom [the Government was] getting the records was a terrorist or a spy. So, you had to already know that the target was a bad guy before you could get the records that would facilitate making that determination.¹¹⁷

After the PA, the standard was changed "to a requirement that the records sought simply need to be relevant to a national security investigation."¹¹⁸

2. *New uses of National Security Letters Pursuant to the PA*

"Criticized for failure to detect the Sept. 11 plot, the [FBI] now casts a much wider net, using [NSLs] to generate leads as well as to pursue them."¹¹⁹ Casual or accidental contact with a suspect may attract the attention of governmental officials subjecting that person to scrutiny about which he may never learn.¹²⁰ Nevertheless, even the FBI has been unable to find a clear example where their expansive use of NSLs has made Americans safer.¹²¹ The unknown efficacy of NSLs did not prevent then Attorney General John D. Ashcroft from revising the Justice Department Guidelines on May 30, 2002 and October 31, 2003, to allow the FBI to retain all information acquired via NSLs.¹²² The authorization included recommendations to develop data mining techniques to make use of such information and freely share pertinent information with any other governmental agency.¹²³

On December 21, 2003, the United States Homeland Security Department declared an "orange" terrorist alert due to intelligence that "hinted" at a New

115. *Id.*

116. *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 483 (S.D.N.Y. 2004).

117. Valerie Caproni, *Symposium: Crimes, War Crimes, and the War on the War on Terror*, 11 LEWIS & CLARK L. REV. 1087, 1095 (2007) (Valerie Caproni, general counsel for the FBI from 2003 to present).

118. *Id.* An additional change made by the PA was that instead of having all NSLs signed by a high ranking official at FBI Headquarters, a special agent in charge of the field office could provide the requisite signature. *Id.*

119. Barton Gellman, *The FBI's Secret Scrutiny*, WASH. POST, Nov. 6, 2005, at A01, available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html>.

120. *Id.*

121. *See id.* ("Michael Mason, who runs the Washington field office and has the rank of assistant FBI director, found no ready answer [to whether expanded flexibility in the use of NSLs have helped]. 'I'd love to have a made-for-Hollywood story, but I don't have one,' Mason said. 'I am not even sure such an example exists.' What national security letters give his agents, Mason said, is speed.")

122. *Id.*

123. *Id.*

Year's Eve attack in Las Vegas, Nevada.¹²⁴ Then FBI Chief in Las Vegas, Ellen Knowlton, received information from FBI headquarters that Al Qaida "could have an interest in Las Vegas, possibly over the New Year's weekend."¹²⁵ This limited information prompted Knowlton to contact the security chiefs of all major casinos and request all information they had on their customers.¹²⁶ After some "arm-twisting" the casinos capitulated to the demand.¹²⁷ This "arm-twisting" came in the form of an NSL.¹²⁸ Due to the new provisions in the PA, NSLs could now be expanded to include a request for an entire database rather than information on a particular individual.¹²⁹

"An interagency task force began pulling together the records of every hotel guest, everyone who rented a car or truck, every lease on a storage space, and every airplane passenger who landed in the city."¹³⁰ After all was said and done, there were no suspected terrorists found in Las Vegas and the information that launched the wide investigation was based upon a mistaken interpretation of a suspected terrorist's communication.¹³¹ Yet, all information obtained in Las Vegas that week has since remained in Federal data banks.¹³²

3. *Independent Executive Action*¹³³

In response to the 9/11 attacks, President George W. Bush created the Terrorist Surveillance Program ("TSP"), which allowed the NSA to intercept phone calls and e-mails traveling in and out of the country in which one party had suspected ties to Al Qaeda.¹³⁴ John Yoo, former Deputy Assistant Attorney General authorized a program titled "The Crown Jewel," which allowed eavesdropping on Americans' international communications without a warrant.¹³⁵ This required data mining *billions* of phone calls and e-mails captured by the NSA.¹³⁶

124. *Id.*

125. *Frontline: Spying on the Home Front* (PBS television broadcast May 15, 2007) [hereinafter *Home Front*] (transcript available at <http://www.pbs.org/wgbh/pages/frontline/homefront/etc/script.html>).

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. Gellman, *supra* note 119, at A01.

131. *Home Front*, *supra* note 125.

132. Gellman, *supra* note 119, at A01.

133. During the cold war, the NSA was only allowed to eavesdrop on international communications; however, this restriction on the NSA's abilities to surveil American citizens' communication was removed by President George W. Bush when he implemented the warrantless wiretap program. *Home Front*, *supra* note 125.

134. *Am. Civil Liberties Union v. Nat'l Sec. Agency*, 438 F. Supp. 2d 754, 758 (E.D. Mich. 2006); Press Release, Press Briefing by Attorney General Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html>; see also Barton Gellman et al., *Surveillance Net Yields Few Suspects*, WASH. POST, Feb. 5, 2006 at A01 [hereinafter Gonzales Press Release], available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html> (stating President Bush described the warrantless program as "terrorist surveillance").

135. *Frontline: Cheney's Law* (PBS television broadcast Oct. 16, 2007) [hereinafter *Cheney's Law*] (transcript available at <http://www.pbs.org/wgbh/pages/frontline/cheney/etc/tapes.html>).

136. *Id.*

Though the NSA is an expert agency in electronic communications, the staggering monitoring ability required to implement the TSP required assistance from the private sector.¹³⁷ In fact, the NSA contracted with AT&T, Verizon, and BellSouth to have access to their subscribers' communications.¹³⁸ The NSA "reached agreements with major American telecommunications companies to gain access to some of the country's biggest 'switches' carrying phone and e-mail traffic into and out of the country."¹³⁹

Though very little is known on how the NSA technically accessed these "switches," one such example has become publicly known.¹⁴⁰ In 2002, the NSA designated a secret room within AT&T's San Francisco office with extensive networking equipment designed to listen to all Internet and telephone communications from all of AT&T's subscribers' communications.¹⁴¹ Mark Klein, a former AT&T technician who discovered the NSA room, brought his findings to the Electronic Frontier Foundation ("EFF").¹⁴² During the investigation of Mark Klein's complaint the EFF discovered, via testimony by Scott Marcus, a former Federal communications expert, that AT&T had set up similar NSA spying rooms in an estimated fifteen to twenty sites across the country.¹⁴³ This alone was enough to intercept 10 percent of *all* domestic Internet traffic in the United States.¹⁴⁴ This prompted EFF to file a lawsuit against AT&T in 2006 seeking to enjoin AT&T from handing over customer information to the NSA.¹⁴⁵

The TSP was completely independent of FISA¹⁴⁶ and was justified by the Bush Administration as being necessary to prevent future terrorist attacks on American soil.¹⁴⁷ Further, Mr. Yoo defended the Executives Branch's use of

137. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, available at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

138. *Id.* The NSA sought to establish a similar arrangement with Qwest Communications; however, the NSA was unsuccessful in convincing Qwest that the proposed action was legal and was denied access to Qwest's networking equipment. *Id.* In addition, both BellSouth and Verizon denied handing over any information to the NSA, however, no representatives from those organizations have been compelled to testify to that fact in front of Congress. *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, at 2A, available at http://www.usatoday.com/news/washington/2006-06-30-nsa_x.htm.

139. Eric Lichtblau, *Bush Defends Spy Program and Denies Misleading Public*, N.Y. TIMES, Jan. 2, 2006, at A11, available at <http://www.nytimes.com/2006/01/02/politics/02spy.html>.

140. *Home Front*, *supra* note 125; see also *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 989 (N.D. Cal. 2006).

141. *Home Front*, *supra* note 125. This equipment included a Narus STA 6400, created by the Narus Corporation, designed with the computational power to monitor millions of electronic communications simultaneously. *Id.*

142. *Id.*

143. *Id.*

144. *Id.*

145. *Hepting*, 439 F. Supp. 2d 974, 979–80.

146. John Yoo, Justice Department Sr. Attorney from 2001 to 2003, responded to accusations that the President violated FISA by not seeking permission from a FISA Court by claiming the President's executive wartime powers granted in the constitution supersede any congressional restraint. *Home Front*, *supra* note 125. Yoo further explained that FISA is not capable of allowing a blanket "driftnet" of electronic data mining on all communications, which, according to Yoo, is necessary when the government has limited information about the parties or nature of the communication. *Id.*

147. Gonzales Press Release, *supra* note 134 (Air Force Gen. Michael V. Hayden stated "There's always a balancing between security and liberty. We understand that this is a more—I'll use the word 'aggressive' program than would be traditionally available under FISA. It is also less intrusive. It deals only with

the program by saying that Congress can no more regulate the President's intelligence gathering techniques than they can regulate where he places troops on the battlefield.¹⁴⁸ The Bush Administration justified the program by claiming that the Authorization to Use Military Force Act of 2001 ("AUMF") provides requisite, albeit implicit, Congressional authority.¹⁴⁹ In addition, the Executive Branch has also proclaimed that legitimate authority for the TSP is found among the inherent powers prescribed in Article II of the United States Constitution.¹⁵⁰

The TSP was reauthorized every forty-five days by then Attorney General John Ashcroft. The program went unabated for two years until Ashcroft fell ill with pancreatitis in 2004.¹⁵¹ This made Jim Comey the acting Attorney General, thus giving him the authority to reauthorize the program.¹⁵² When Comey refused to renew the program, Alberto Gonzales, then White House Counsel, rushed to the hospital in which Ashcroft was staying in order to persuade Ashcroft to reauthorize the program.¹⁵³ Ashcroft rose from the bed and made a clear and inspiring speech explaining why he would not approve the program, and he stated he had no authority to do so anyway because Jim Comey was legally the new acting Attorney General.¹⁵⁴ Nevertheless, the next morning President Bush reauthorized the program on his own signature.¹⁵⁵ This outrageous conduct prompted the current FBI Chief Robert Mueller to

international calls. It is generally for far shorter periods of time. And it is not designed to collect reams of intelligence, but to detect and warn and prevent about attacks. And, therefore, that's where we've decided to draw that balance between security and liberty.").

148. *Cheney's Law*, *supra* note 135.

149. David Cole, *Reviving the Nixon Doctrine: NSA Spying, the Commander-in-Chief, and Executive Power in the War on Terror*, 13 WASH. & LEE J. CONST. RTS. & SOC. JUST. 17, 21 (2006). The Authorization for use of Military Force states in part:

Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States

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

150. John Sims, *What NSA Is Doing . . . and Why It's Illegal*, 33 HASTINGS CONST. L.Q. 105, 133 (2006).

151. *Cheney's Law*, *supra* note 135.

152. *Id.*

153. *Id.*

154. *Id.*

155. *Id.*; *see also* President's Radio Address, Office of the Press Secretary, Dec. 17, 2005, available at <http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html>. President George W. Bush stated:

The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for as long as our nation faces a continuing threat from al Qaeda and related groups. The NSA's activities under this authorization are thoroughly reviewed by the Justice Department and NSA's top legal officials, including NSA's general counsel and inspector general.

Id.

threaten President Bush with his immediate resignation unless Bush changed the program.¹⁵⁶ Ostensibly acquiescing to Mueller's demands, Bush modified the program to the satisfaction of Mueller.¹⁵⁷ The change remains top secret to date.¹⁵⁸

In 2005, a Department of Justice legal opinion written by the Office of Legal Counsel, which remains secret to date, gave the CIA the same latitude of that in "The Crown Jewel" program.¹⁵⁹ These activities prompted the newly elected Democrats of 2006 from both the House and Senate to inquire into aforementioned warrantless wire-tapping activity by the Executive Branch.¹⁶⁰ Congress's attempt to subpoena the Vice-President was quelled by his invocation of executive privilege.¹⁶¹ This led to Gonzales's appearance before the Senate and his subsequent resignation as Attorney General.¹⁶²

4. *The USA PATRIOT Improvement and Reauthorization Act of 2005*

On March 9, 2006, Congress passed the USA PATRIOT Improvement and Reauthorization Act Of 2005 ("PA II") due to a sunset provision in the PA mandating an automated repeal.¹⁶³ In addition to the reauthorization, Congress also amended certain provisions within the PA to resolve certain "as applied" ambiguities.¹⁶⁴

First, rather than the complete prohibition on disclosure of an NSL, as found in PA, PA II applies a case-by-case analysis that requires the FBI to certify that disclosure "[m]ay result . . . [in] danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person."¹⁶⁵ Further, a recipient of an NSL can petition a United States district court to modify or set aside the

156. *Cheney's Law*, *supra* note 135.

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*

163. USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat 192 (2006).

164. *See generally* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (analyzing ISP's constitutional challenge of section 2709, and holding that the FBI's demand for "compulsory, secret, and unreviewable production of information" violates the Fourth Amendment). "The NSL statutes, particularly § 2709, present interpretive challenges in at least three respects, the first two of which have a direct bearing on the motions now before the Court. First, while two of the NSL statutes explicitly state that an NSL recipient may disclose the Government's inquiry to persons whose assistance is necessary to comply with the demands of the NSL, the other statutes, including § 2709, appear by their telltale silence on that point, to preclude any disclosures. None of the statutes explain whether consulting an attorney constitutes disclosure, even where an attorney's assistance may be necessary for a recipient to comply with an NSL, and none of the statutes states whether the ban on disclosure may ever be lifted by a court. Second, the statutes contain no explicit provision for the Government to seek judicial enforcement of an NSL against a recipient who refuses to comply, nor is there any provision expressly authorizing an NSL recipient to affirmatively challenge, administratively or judicially, the propriety of an NSL request. Third, there is no explicit provision in the statutes imposing penalties against a person who fails to comply with an NSL." *Id.* at 492.

165. 18 U.S.C.A. § 2709(c) (Supp. 2008).

request “if compliance would be unreasonable, oppressive, or otherwise unlawful.”¹⁶⁶ This ability to petition, and seek to modify or set aside, also extends to a nondisclosure requirement.¹⁶⁷ However, if an FBI official certifies that a disclosure “may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive unless the court finds that the certification was made in bad faith.”¹⁶⁸

Second, PA II distinguishes between petitions filed within a year and those filed outside a year’s time after receipt. Specifically, if a petition to modify or set aside a nondisclosure requirement is filed within a year, the court may grant relief only if there is no reason to believe the disclosure would endanger national security.¹⁶⁹ If the petition is filed after one year of receipt of an NSL, the FBI has the option of re-certifying the nondisclosure request if it is based upon national security concerns.¹⁷⁰ Nonetheless, if the reviewing court denies a petition to modify or set aside a nondisclosure request, the recipient is prevented from filing another petition for one year.¹⁷¹ Notwithstanding such prophylactic constitutional provisions found within PA II, it still does not obviate constitutional criticism.¹⁷²

III. ANALYSIS

The electronic surveillance that the United States Government has participated in post-9/11 implicates several constitutional principles: namely, the First Amendment, Fourth Amendment, and the constitutional doctrine of separation of powers.¹⁷³

As stated by the First Amendment and Supreme Court decree, if a statute allows for any governmental discretion in limiting speech, like that found in the PA and PA II, such discretion must be subject to objective standards.¹⁷⁴ Regarding the Fourth Amendment, the Executive has relied upon AUMF and Article II to argue it has the constitutional authority to operate the TSP.¹⁷⁵ However, current statutes already provide contingencies for a state of war; nevertheless, there has been no official declaration of war.¹⁷⁶ Furthermore, the Supreme Court has explicitly stated that the Executive Branch cannot circumvent the Fourth Amendment even in a time of war.¹⁷⁷

According to the constitutional doctrine of separation of powers, the Executive Branch’s authority is greatest when Congress explicitly allows an

166. *Id.* § 3511(a).

167. *Id.* § 3511(b).

168. *Id.*

169. *Id.*

170. *Id.*

171. *Id.*

172. *See infra* Part III.

173. *See infra* Part III.

174. *See infra* Part III.A.

175. *See infra* Part III.B.

176. *See infra* Part III.B.

177. *See infra* Part III.B.

action, and it is at its lowest ebb when the Executive Branch takes any action incompatible with the expressed or implied will of Congress.¹⁷⁸ In addition, the Executive Branch must respect the Judicial Branch's constitutional authority, and any attempt by the Executive Branch to limit judicial review and discretion is an infringement upon such authority.¹⁷⁹

A. First Amendment

The First Amendment of the United States Constitution states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech"¹⁸⁰ This fundamental right cannot easily be dispensed with, and when Congress implements a statute allowing governmental discretion to limit speech, that discretion must be limited by objective criteria.¹⁸¹

Both the PA and PA II allow governmental discretion in the administration of a nondisclosure request; thus, they must be limited by objective criteria.¹⁸² The Supreme Court of the United States has devised a test when such discretion is present, in order to prevent the dangers associated with censorship.¹⁸³ This test, known as the *Freedman* test, states:

[t]he government must exercise its discretion within a system that allows for "procedural safeguards designed to obviate the dangers of a censorship system." . . . (1) any restraint in advance of judicial review may be imposed only for "a specified brief period," (2) any further restraint prior to "a final judicial determination on the merits" must be limited to "the shortest fixed period compatible with sound judicial resolution," and (3) the burden of going to court to suppress the speech and the burden of proof once in court must rest on the censoring government.¹⁸⁴

Prior to PA II, both the first and second factors under the *Freedman* test would have likely failed; however, changes made in PA II implemented additional judicial safeguards not present in PA.¹⁸⁵ Even so, the third factor of the *Freedman* test still is not satisfied under the newly enacted PA II.¹⁸⁶ Particularly, factor three of the *Freedman* test requires that the burden of proof in the suppression of speech rest upon government.¹⁸⁷ Problematically, title 18, section 2709(c) of the United States Code "[g]rants broad discretion to the FBI to completely restrict constitutionally protected speech on the basis of its

178. See *infra* Part III.C.

179. See *infra* Part III.C.

180. U.S. CONST. amend. I.

181. *Doe v. Gonzales*, 500 F. Supp. 2d 379, 399 (S.D.N.Y. 2007).

182. 18 U.S.C.A. § 2709(c) (Supp. 2008); see also *Gonzales*, 500 F. Supp. 2d at 399 (stating that objective criteria is required).

183. *Freedman v. Maryland*, 380 U.S. 51, 58–59 (1965).

184. *Gonzales*, 500 F. Supp. 2d at 399 (citing *Freedman*, 380 U.S. at 58–59).

185. See *id.* at 401 (stating the reason that PA II satisfies factor one and two of the *Freedman* test is due to the additional judicial safeguards that were not present in PA).

186. *Id.* at 405.

187. *Id.* at 401.

content, and it places the burden of challenging this restriction in court solely on the NSL recipient”¹⁸⁸

The government’s response to First Amendment criticism focuses largely on ostensibly analogous statutes that have avoided abrogation by the courts.¹⁸⁹ In particular, the government focuses on statutes that allow it to apply wiretaps, pen registers, and FISA subpoenas.¹⁹⁰ To bolster this argument, these statutes also do not have the same broad ability of judicial review as that prescribed by the PA II.¹⁹¹ However, those statutes differ from those prescribing use of NSLs because the court authorizes the search *ex ante* and provides judicial safeguards after the search has concluded.¹⁹² Additionally, both the wiretap and pen register statutes “impl[y] that communications providers might be free to discuss wiretaps and pen registers, as well as their knowledge of underlying criminal investigations, after those investigations are completed.”¹⁹³

The ability of the government to restrict speech in grand jury cases well after the time period in which it was necessary has also been found to be unconstitutional.¹⁹⁴ A law prohibiting grand jury witnesses from disclosing their testimony after the jury term has ended violates the First Amendment to the United States Constitution.¹⁹⁵ On the other hand, a law preventing grand jury witnesses from revealing their testimony post-jury term is acceptable, so long as the criminal investigation of the crime continues.¹⁹⁶ Conversely, the revisions provided by PA II regarding NSLs “[c]ontinues to authorize nondisclosure orders that *permanently* restrict an NSL recipient from engaging in *any* discussion related to its receipt of the NSL,” thus, violating the First Amendment.¹⁹⁷

1. *Executive Action Post-9/11 and the First Amendment*¹⁹⁸

England’s history of the freedom of speech and press is intertwined with the scope of a search and seizure.¹⁹⁹ “This history was, of course, part of the

188. *Id.* at 405.

189. *Id.* at 392.

190. 18 U.S.C. § 2511(2)(a)(ii) (2000) (wiretaps); *id.* § 3123(d)(2) (pen registers); 50 U.S.C. § 1861(d) (2000) (FISA).

191. *Gonzales*, 500 F. Supp. 2d at 392.

192. *Id.* at 393.

193. *Id.*

194. *Butterworth v. Smith*, 494 U.S. 624, 626 (1990).

195. *Id.*

196. *Hoffmann-Pugh v. Keenan*, 338 F.3d 1136, 1137 (10th Cir. 2003).

197. *Gonzales*, 500 F. Supp. 2d at 420 (emphasis in the original).

198. *See generally* Am. Civil Liberties Union v. Nat’l Sec. Agency, 438 F. Supp. 2d 754, 775 (E.D. Mich. 2006) (analyzing the legality of an NSA secret program in which the government intercepted international telephone and Internet communications without a warrant).

199. *See generally* *Marcus v. Search Warrants of Prop.*, 367 U.S. 717, 724–26 (1961) (“Each succeeding regime during turbulent Seventeenth Century England used the search and seizure power to suppress publications. James I commissioned the ecclesiastical judges comprising the Court of High Commission ‘to enquire and search for . . . all heretical, schismatical and seditious books, libels, and writings, and all other books, pamphlets and partraitures offensive to the state or set forth without sufficient and lawful authority in that behalf . . . and the same books (etc.) and their printing-presses themselves likewise to seize and so to order

intellectual matrix within which our own constitutional fabric was shaped. The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression.”²⁰⁰

The TSP created by the Executive Branch may be one such instance where the government’s ability to search electronic communications will have a direct impact on one’s proclivity to freely express himself or herself.²⁰¹ Though this observation may seem hyperbolic, “[h]istory abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. . . . [P]rotections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.”²⁰²

*B. Fourth Amendment*²⁰³

“[T]he warrant requirement [within the Fourth Amendment] has been a valued part of our constitutional law for decades It is not an inconvenience to be somehow ‘weighed’ against the claims of police efficiency.”²⁰⁴

1. Executive Action Post-9/11 and the Fourth Amendment

The warrant requirement is an important functional element of restrained governance to prevent even well-intentioned, yet over-enthusiastic, governmental officials, from exceeding their constitutional boundaries.²⁰⁵ Yet, the aforementioned TSP was created because the Executive Branch believed such efficiencies were necessary, and current surveillance laws inadequate, to protect American citizens from future terrorist attacks.²⁰⁶

The Executive Branch argued this efficiency is necessary in a state of war, which we are currently in.²⁰⁷ Specifically, the Executive Branch stated the Congressional authority to fight against terrorism, as found in AUMF, is all

and dispose of them . . . as they may not after serve or be employed for any such unlawful use”).

200. *Id.* at 729.

201. This assumes the individual uncomfortable freely expressing themselves, due to a program like the TSP, is aware such a program exists.

202. *Am. Civil Liberties Union*, 438 F. Supp. 2d at 776 (citing *United States v. U.S. Dist. Court*, 407 U.S. 297, 313–14 (1972)).

203. Under the PA, Fourth Amendment concerns were legitimate. *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 476 (S.D.N.Y. 2004). Section 2709(c) of title 18 in the United States Code prevented an NSL recipient to “from revealing the existence of an NSL inquiry the FBI pursued under § 2709 in every case, to any person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected, under any circumstances, either by the FBI itself, or pursuant to judicial process.” *Id.* Therefore, section 2709 violated the Fourth Amendment because it barred a judicial challenge to an NSL request. *Id.* at 475. Nevertheless, PA II rectified that procedural deficiency by allowing an NSL recipient to challenge a nondisclosure request. USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat 192 (2006).

204. *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971).

205. *Id.*

206. *See supra* Part II.3.

207. *See supra* Part II.3.

that is needed to justify such an expansive surveillance program.²⁰⁸ However, the AUMF is not a declaration of war, but Congressional “authorization” to use force.²⁰⁹ If the Executive Branch is going to argue it has “war powers” to implement the TSP, should not such an assertion require an actual declaration of war? Furthermore, even if such a declaration were granted by Congress, would that justify the Executive Branch in ignoring a FISA provision (a mere Congressional act) that *explicitly* states what actions are *allowed* by the President in a time of war? If not, how would it be remotely possible for the Executive Branch to have the constitutional authority to disregard the Fourth Amendment?

“[T]he Bill of Rights of the United States Constitution must be applied despite authority granted by the AUMF.”²¹⁰ Significantly, these constitutional restrictions are also applicable to the Executive Branch’s constitutional powers embedded in Article II.²¹¹ If this were not so, then Congress’s attempt to restrain the Executive Branch’s actions during war, as found within FISA, is an unconstitutional Congressional infringement upon Article II.²¹² Hitherto, “[t]here does not appear to be any precedent even vaguely on point – that is, where Congress legislated in an area within its legislative authority and it was nonetheless held by the Supreme Court that the President had inherent authority to act contrary to the statute.”²¹³

The argument that Article II of the United States Constitution allows the Executive Branch to avoid adhering to restrictions within the Bill of Rights, in a time of war, was erroneous when proclaimed by the Nixon Administration and is equally erroneous today.²¹⁴ In fact, the only Supreme Court case addressing the use of wiretaps for national security purposes is *United States v. U.S. District Court*.²¹⁵ In this case, the Supreme Court concluded that domestic electronic surveillance to further the Executive Branch’s obligation to protect national security is insufficient to circumvent the Fourth Amendment.²¹⁶

In summary, the Supreme Court of the United States recently and concisely declared:

Striking the proper constitutional balance here is of great importance to the Nation during this period of ongoing combat. But it is equally

208. See *supra* Part II.3.

209. 50 U.S.C.A. § 1541 (2000).

210. *Am. Civil Liberties Union*, 438 F. Supp. 2d at 780 (citing *Hamdi v. Rumsfeld*, 542 U.S. 507, 532, 537 (2004)).

211. See *Hamdi*, 542 U.S. at 516–17 (though the Court did not expressly determine whether Article II does provide such Executive powers, the Court certainly did not appeal to, nor reference, Article II powers in determining that the Executive Branch is subject to the constitutional restrictions found within the Bill of Rights).

212. *Sims*, *supra* note 150, at 129.

213. *Id.* at 133.

214. See *Bloom & Dunn*, *supra* note 69, at 149 (“The comparison between the actions taken by President George W. Bush and Richard M. Nixon are not merely academic but are unnervingly similar in substance, scope, and perceived authority.”).

215. 407 U.S. 297 (1972); *Bloom & Dunn*, *supra* note 69, at 196.

216. *U.S. Dist. Court*, 407 U.S. at 316–17 (“Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.”).

vital that our calculus not give short shrift to the values that this country holds dear or to the privilege that is American citizenship. It is during our most challenging and uncertain moments that our Nation's commitment to due process is most severely tested; and it is in those times that we must preserve our commitment at home to the principles for which we fight abroad.²¹⁷

C. Separation of Powers

When the Founding Fathers gathered together to create a new nation they did so with the knowledge of history and with the intent to create a government that would restrain itself.²¹⁸ In so doing, they devised a Constitution that created three branches of government with each part assigned distinct functions and requisite powers.²¹⁹ Though each branch was separate, they were coequal and "while independent of the others, the workings of each were integrated as a whole . . . [t]o guarantee that lasting stability demands that each branch honors its own bounds of authority, and those of the others."²²⁰ Succinctly stated, "[o]ur national experience teaches that the Constitution is preserved best when each part of the Government respects both the Constitution and the proper actions and determinations of the other branches."²²¹

Recent legislation sought to rectify constitutional deficiencies and *explicitly* allow the Executive Branch the ability to perform surveillance without a warrant.²²² This legislation, known as the Protect America Act of 2007, was enacted in August 2007 and allowed the Executive Branch to electronically surveil a suspected terrorist reasonably believed to be outside the United States for up to one year without a warrant and provided immunity to telecommunication providers that assisted the government in doing so.²²³ However, Congress was cautious with such a grant of power and built in a sunset provision that automatically nullified the law at the end of 180 days if there was no subsequent congressional action.²²⁴ Congress did not act and the law sunset February 17, 2008.²²⁵ Nevertheless, notwithstanding Congressional prudence to build in a sunset provision, such explicit authorization does not ameliorate the aforementioned constitutional criticism.²²⁶

217. *Hamdi v. Rumsfeld*, 542 U.S. 507, 532 (2004).

218. *Doe v. Gonzales*, 500 F. Supp. 2d 379, 409–10 (S.D.N.Y. 2007).

219. *Id.* at 410.

220. *Id.*

221. *City of Boerne v. Flores*, 521 U.S. 507, 535–36 (1997).

222. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

223. *Id.*

224. *Id.*

225. See generally Pamela Hess, *Bush Says Congress Putting US in Danger*, HUFFINGTON POST, Feb. 15, 2008, http://www.huffingtonpost.com/2008/02/15/bush-says-congress-puttin_n_86811.html (reporting that the eaves drop law was on the verge of expiration and discussing its implications).

226. See Part III.A–B.

1. Executive Encroachment on the Legislative

a. Authority Not Found Within FISA

The Constitution of the United States provides the President with the power that “[h]e shall take care that the laws be faithfully executed.”²²⁷ Even so, James Madison warned that “[t]he accumulation of all powers, legislative, executive, and judiciary, in the same hands, whether of one, a few, or many, and whether hereditary, self-appointed, or elective, may justly be pronounced the very definition of tyranny.”²²⁸

When determining what authority a President retains when implementing congressional acts, whether implicit or explicit, the seminal Supreme Court case is *Youngstown Sheet & Tube Co. v. Sawyer*.²²⁹ In this case, the question for the Court was whether President Harry Truman, during the Korean War, could nationalize all steel mills throughout the United States without Congressional consent (use law-making powers).²³⁰ In determining that the President had no such power, the Supreme Court noted that “[t]he President’s power . . . must stem either from an act of Congress or from the Constitution itself.”²³¹ In particular, there was no statute that expressly authorized the President’s action, nor an act of Congress that could fairly imply such power.²³²

Conversely, if the President acts when a statute expressly or implicitly grants such power, “his authority is at its maximum.”²³³ It is only in these circumstances that the President can be said to personify complete federal sovereignty.²³⁴ Yet, “[w]hen 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 own constitutional powers minus any constitutional powers of Congress”²³⁵ Regarding the TSP, the Executive Branch has implemented a system of surveillance that FISA expressly forbids.²³⁶ Specifically, FISA allows for a special executive procedure in times of war.²³⁷ Thus, the TSP constitutes an action by the Executive Branch when its authority is at its lowest ebb.²³⁸

The concept explicated within the Constitution that the President must see that the law be faithfully executed is conclusive proof that the President is *not* a lawmaker.²³⁹ The law-making power granted to Congress within the

227. U.S. Const. art. II, § 3.

228. THE FEDERALIST NO. 47 (James Madison).

229. *Am. Civil Liberties Union v. Nat’l Sec. Agency*, 438 F. Supp. 2d 754, 777 (E.D. Mich. 2006).

230. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 583 (1952).

231. *Id.* at 585.

232. *Id.*

233. *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

234. *Id.* at 635–36.

235. *Id.* at 637.

236. *Am. Civil Liberties Union v. Nat’l Sec. Agency*, 438 F. Supp. 2d 754, 778 (E.D. Mich. 2006).

237. 50 U.S.C. § 1811 (2000).

238. *Am. Civil Liberties Union*, 438 F. Supp. 2d at 778.

239. *Youngstown*, 343 U.S. at 587.

Constitution is not subject to presidential or military supervision or control.²⁴⁰ To conclude, “[w]ith all its defects, delays and inconveniences, men have discovered no technique for long preserving free government except that the Executive be under the law, and that the law be made by parliamentary deliberations.”²⁴¹

b. Authority Not Found Within AUMF

The AUMF allows for the President to use all necessary and appropriate force against those who aided or were associated with the terrorist attacks of 9/11, in order to prevent another terrorist attack from transpiring.²⁴² The Executive Branch relies upon the AUMF as the statute passed by Congress that implicitly allows for the implementation of the TSP.²⁴³

Yet, “FISA and Title III, are together by their terms denominated by Congress as the exclusive means by which electronic surveillance may be conducted” and those statutes clearly state that a warrant must be obtained to conduct electronic surveillance and that any stated exception within is not applicable to the TSP.²⁴⁴ The general powers granted in the AUMF are subversive to the detailed and specific powers found within FISA and Title III.²⁴⁵ Glaringly, the “AUMF was adopted without there being any reference to [the] NSA, to its mission, to the targeted interception of international communications of United States persons within the United States, or to any aspect of FISA.”²⁴⁶

The government had the opportunity to convince the Supreme Court that the AUMF granted powers to the Executive Branch to indefinitely detain an enemy combatant.²⁴⁷ The Court agreed with the Executive Branch that the ability to capture and detain an enemy combatant was implied by AUMF.²⁴⁸ However, the Court disagreed with the government that this implication was meaningful enough to deny the detainee the constitutional right to be brought before a neutral magistrate.²⁴⁹ Accordingly, “the Bill of Rights of the United States Constitution must be applied despite authority granted by the AUMF.”²⁵⁰

2. Executive and Legislative Encroachment on the Judiciary

Due to the reforms prescribed by PA II, title 18, section 3511(b)(2) of the

240. *Id.* at 588.

241. *Id.* at 655 (Jackson, J., concurring).

242. *See generally* Authorization for Use of Military Force Against Iraq, Pub. L. No. 107-243, 116 Stat. 1498 (2002) (describing justification for powers).

243. *See supra* Part II.B.3. *See generally* *Am. Civil Liberties Union*, 438 F. Supp. 2d at 779 (arguing that the AUMF gave the government the authority to implement the TSP).

244. *Am. Civil Liberties Union*, 438 F. Supp. 2d at 779.

245. *Id.* (citing *Morales v. TWA, Inc.*, 504 U.S. 374, 384 (1992)).

246. *Sims, supra* note 150, at 132.

247. *Hamdi v. Rumsfeld*, 542 U.S. 507, 510 (2004).

248. *Id.* at 519.

249. *Id.* at 533.

250. *Am. Civil Liberties Union*, 438 F. Supp. 2d at 780 (citing *Hamdi*, 542 U.S. at 532, 537, 572).

United States Code states that “[i]f, at the time of the petition [to review a nondisclosure request], the Attorney General . . . certifies that disclosure may endanger the national security of the United States . . . such certification shall be treated as conclusive.”²⁵¹ The only exception to this provision is if the court finds that the certification was made in bad faith.²⁵²

Section 3511(b)(2) prescribes the standard of review that a court must adhere to when determining the propriety of a nondisclosure request. Further, when a statute places a prior restraint on speech, it will be strictly construed to ensure it is narrowly tailored to advance a compelling governmental interest.²⁵³ This standard, developed by the Judicial Branch, is applicable to the other branches of government.²⁵⁴ When the Judiciary has stated what the constitutional law is, Congress is not endowed with the power to proclaim that a constitutional standard is something else.²⁵⁵ Even so, that is exactly what section 3511(b)(2) purports to do by decreasing the standard of review and level of deference the Judiciary rightfully retains in determining the propriety of a nondisclosure request.²⁵⁶

Notably, the revisions approbated by PA II could set a precedent that it is acceptable for the Executive or Legislature to encroach upon the discretionary realm of the Judiciary.²⁵⁷ Though such a step by the Legislature may seem innocuous, such a course “could later stretch into a means of farther and more detrimental invasion of the courts’ prerogatives—the legislative equivalent of breaking and entering, with an ominous free pass to the hijacking of constitutional values.”²⁵⁸ The requirement that the Judicial Branch find the Executive’s claim of national security “conclusive,” outside evidence of bad faith, removes any meaningful judicial review and obligates the Judiciary to uncritically accept the government’s commitment to the ostensible need for secrecy.²⁵⁹

The Judicial Branch’s befitting jealous guard over its prerogative must not be understated.²⁶⁰ Obligating it to accept the Executive’s certification of a nondisclosure request as conclusive allows the Executive Branch to determine the constitutionality of its own actions.²⁶¹ Accordingly:

[if] Congress were able . . . to prescribe the precise corresponding rule telling the courts what level of scrutiny to apply in properly gauging the constitutionality of the statute’s application . . . separation and balance of powers . . . could be severely compromised . . . with consequential diminution of the judiciary’s function, and hence

251. 18 U.S.C.A. § 3511(b)(2) (Supp. 2008).

252. *Id.*

253. *United States v. Playboy Ent. Group, Inc.*, 529 U.S. 803, 813 (2000).

254. *Id.*

255. *Doe v. Gonzales*, 500 F. Supp. 2d 379, 412 (S.D.N.Y. 2007).

256. *Id.*

257. *Id.* at 413.

258. *Id.*

259. *Id.* at 419.

260. *See id.* (“In requiring the Court to accept the government’s certification as conclusive, § 3511(b) effectively allows the government to determine the constitutionality of its own actions . . .”).

261. *Id.*

potential dire effects to individual freedoms.²⁶²

IV. RECOMMENDATION

“[C]ongress, even once apprised (and aghast) about a massive electronic surveillance program, cannot easily act. So long as the president claims to ground his surveillance program in some law, no matter how dubious, it will require Congress to pass a new law to trump that interpretation.”²⁶³ Due to congressional concern over the Executive Branch’s potential abuse of authority post-September 11, 2001, both houses of Congress have decided to rectify the potential constitutional infirmities and have introduced legislation to that effect.²⁶⁴

The title of both the House and Senate Bill is the National Security Letter Reform Act of 2007 (“Reform Act”).²⁶⁵ The Reform Act has several provisions that seek to address aforementioned criticisms found within this Note. This Act, with a few additional modifications, resolves First and Fourth Amendment concerns and restores the Judicial Branch’s constitutional prerogative to oversee the other branches of government. Accordingly, it is recommended that Congress enact the Reform Act, albeit with a few additional ancillary and constitutional prophylactic measures.

A. Fourth Amendment Protections Restored

As previously stated, neither AUMF nor Article II of the United States Constitution precludes application of the Bill of Rights.²⁶⁶ Unfortunately, arguments by the Executive Branch that AUMF or Article II provide the necessary powers to conduct warrantless surveillance could potentially remain, even if subsequent legislation is enacted that disallows such conduct.²⁶⁷ However, this does not render the Reform Act powerless in this regard. The Reform Act’s provisions provide certain restrictions that could potentially make it difficult for the Executive Branch to abuse both FISA and the use of NSLs.

1. FISA Restrictions

The Reform Act has a powerful provision that provides a private cause of action against an electronic communications provider that does not carefully

262. *Id.* at 413.

263. Neal Kumar Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent* 102–56 (2005) (Faculty Working Paper, Georgetown Law), available at <http://ssrn.com/abstract=1101577>.

264. National Security Letters Reform Act of 2007, H.R. 3189, 110th Cong. (2007); National Security Letter Reform Act of 2007, S. 2088, 110th Cong. (2007).

265. There is actually a slight variation with the Senate bill named National Security Letters Reform Act and the House bill National Security Letter Reform Act. S. 3189; H.R. 3189. Considering both bills are fairly similar, reference to the sections therein will be made to the superior provision provided between the two.

266. *See supra* Part III.B.

267. This is so because the Executive Branch’s argument is predicated upon the doctrine of separation of powers, not that the legislature has explicitly granted warrantless surveillance. *See supra* Part III.C.

follow the law. It states:

A person to whom records requested by an [NSL] pertains may, in a civil action against any person issuing or obtaining the issuing of such letter, obtain money damages equal to the greater of the actual damages or \$50,000, if the [NSL] was issued contrary to law or the certification on which it was based was without factual foundation.²⁶⁸

Though this specifically pertains to NSLs, this is one area where such liability should also be extended to private-sector violations of pertinent FISA provisions. To the consternation of the Bush Administration, such a modification of FISA would make the NSA warrantless surveillance much more difficult.²⁶⁹ This is because the NSA heavily depends on the capabilities and equipment of the private sector.²⁷⁰ President Bush stated “[w]ithout this [private-sector] protection, without this liability shield, we may not be able to secure the private sector’s cooperation with our intelligence efforts. And that, of course, would put the American people at risk.”²⁷¹

The claim by the President that American citizens may be at risk if private-sector liability is allowed may be countered by the fact that such liability may only be found if the electronics communications provider knowingly allows the government to violate the law. However, such a standard is only applicable and appropriate if the electronics communication provider has some ability to review particular FISA requests made by the government. As a result, the PA II provisions allowing the government to install its own electronic equipment on the provider’s premises may also need to be repealed.²⁷²

Though this approach may seem drastic, it will still retain the prior FISA restrictions shown to be effective for nearly 30 years. Particularly, “[t]he Federal Intelligence Surveillance Court . . . itself has been very willing to grant warrants, issuing all but 6 of the 20,000 requests made by the government.”²⁷³ More importantly, this prophylactic measure will provide a check against the Executive Branch’s ability to violate the Fourth Amendment while avoiding procedural difficulties in monitoring the government’s actions.

2. NSL Restrictions

The Executive Branch has also neglected the Fourth Amendment standard of individual suspicion when it sought to use NSLs to request an entire database of information, rather than information on a particular individual.²⁷⁴

To restore the standard of individual suspicion, the Reform Act provides that an NSL must contain “specific and articulable facts providing reason to

268. H.R. 3189, § 4.

269. President George W. Bush, Address from White House South Lawn (Feb. 14, 2008).

270. *Id.*

271. *Id.*

272. See 18 U.S.C.A. § 3123 (Supp. 2008).

273. Zmarak Khan, *The National Security Agency (NSA) Eavesdropping on Americans: A Programme that Is Neither Legal nor Necessary*, 2.2 UTRECHT L. REV. 61, 78 (Dec. 2006).

274. *Home Front*, *supra* note 125.

believe that the records” pertain to an *individual*.²⁷⁵ That is, the individual must be a suspected agent of a foreign power or “pertain to an individual who has been in contact with, or otherwise directly linked to, a suspected agent of a foreign power.”²⁷⁶ The NSL provision, within the PA, states the government may acquire information about an *entity* that is *relevant* to an ongoing investigation.²⁷⁷

Further protections within the Reform Act relate to *what* the government can acquire. In particular, the Reform Act allows the government the ability to acquire only:

(A) The name of the customer or subscriber. (B) The address of the customer or subscriber. (C) The length of the provision of service by such provider to the customer or subscriber (including start date) and the types of service utilized by the customer or subscriber. (D) The telephone number or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address. (E) The means and sources of payment for such service (including any credit card or bank account number). (F) Information about any service or merchandise orders, including any shipping information and vendor locations. (G) The name and contact information, if available, of any other wire or electronic communications service providers facilitating the communications of the customer or subscriber.²⁷⁸

Conversely, the PA requires an electronic communications provider to “comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession.”²⁷⁹

The Reform Act’s explicit enumeration of what can be acquired avoids inherent ambiguities found within the PA provision. To bolster this argument, the Reform Act explicitly states that NSLs “issued pursuant to this section shall not require the production of local or long distance telephone records or electronic communications transactional information not listed.”²⁸⁰ Accordingly, these modifications allow the government little room to apply an NSL to an entire database and ideally prevent the government from acquiring broad categories of information.

B. First Amendment Protections and Judicial Overview Restored

As previously discussed, PA II remedied several constitutional deficiencies found within the PA, but not all. Thus, three constitutional deficiencies remain. First, the recipient of a nondisclosure request bears the

275. National Security Letter Reform Act of 2007, S. 2088, 110th Cong. § 2(b) (2007).

276. *Id.*

277. 18 U.S.C. § 2709(b).

278. S. 3189, § 2(a)(1).

279. 18 U.S.C. § 2709(a).

280. S. 3189, § 2(a)(2).

burden of proof that the government is unreasonably suppressing speech.²⁸¹ Second, NSLs “[c]ontinue[] to authorize nondisclosure orders that *permanently* restrict an NSL recipient from engaging in *any* discussion related to its receipt of the NSL.”²⁸² Third, “[i]f, at the time of the petition [to review a nondisclosure request], the Attorney General . . . certifies that disclosure may endanger the national security of the United States . . . such certification shall be treated as conclusive.”²⁸³

The Reform Act provides solutions for all three issues. Regarding the suppression of speech via a nondisclosure request, the government “may apply for an order prohibiting disclosure that the Federal Bureau of Investigation has sought or obtained access to information or records under this section *for not more than 180 days* after the order is issued.”²⁸⁴ A further limitation provides that an “[a]pplication for an order pursuant to this subsection must state specific and articulable facts giving the applicant [government] reason to believe that disclosure . . . sought . . . will result in” several specified risks.²⁸⁵ Conveniently, these two provisions also provide safeguards that prevent a nondisclosure request from becoming permanent.²⁸⁶

Regarding judicial review, the Reform Act establishes that “[a] person prohibited by law from disclosing information about the [NSL] may file . . . a petition for the court to set aside the nondisclosure requirement. Such petition . . . may be based upon any failure of the nondisclosure requirement to comply with this section or upon any constitutional or other legal right.”²⁸⁷ Additionally, only the court will have the authority to set aside a nondisclosure requirement.²⁸⁸

V. CONCLUSION

James Madison’s assertion that great difficulties lie in creating a government that controls the citizenry and itself is no less true today. In furtherance of that goal, the main body of the Constitution enumerates three independent, but co-equal, branches of the federal government. Further, the Bill of Rights of the United States Constitution provides several individual liberties the government must respect in the implementation of the law. Among these liberties are an American citizen’s right to speech and privacy, as per the First and Fourth Amendments respectively.

Nonetheless, as early as the Civil War, the United States Government has continually infringed upon those rights via electronic monitoring programs

281. *See supra* Part III.A.

282. *Doe v. Gonzales*, 500 F. Supp. 2d 379, 420 (S.D.N.Y. 2007) (emphasis in the original).

283. 18 U.S.C.A. § 3511(b)(2) (Supp. 2008).

284. National Security Letters Reform Act of 2007, H.R. 3189, 110th Cong. § 3(d)(3) (2007) (emphasis added).

285. *Id.* § 3(d)(5) (stating such risks include “[e]ndangering the life or physical safety of any person; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously endangering the national security of the United States . . .”).

286. *Id.* § 3(d)(3), (5).

287. *Id.* § 3(e)(2)(a).

288. *Id.*

directed towards the general public. Regrettably, this monitoring activity has accelerated since the tragic terrorist attacks against the American public on 9/11. This acceleration has been instigated by the Executive Branch's insistence that such power is found within either the AUMF or Article II of the United States Constitution.

However, constitutional restrictions found within the First Amendment, Fourth Amendment, and the doctrine of separation of powers refute such claims. Additionally, Supreme Court precedent, the history of wartime surveillance in the United States, and principles of statutory construction all fail to sustain the Executive Branch's extraordinary claim of authority.

Accordingly, drastic measures are necessary to control the current power and ability of the Executive Branch while maintaining the tools necessary for the government to protect the American people from a future terrorist attack. In so doing, it is recommended a modified application of the National Security Letters Reform Act of 2007 be adopted by both houses of Congress. If this achievement is realized, it has the potential of restoring First and Fourth Amendment protections, and the Judicial Branch's constitutional authority, which have contributed to the greatness of the United States of America over the past 200 years.