Brooklyn Journal of International Law

Volume 29 | Issue 1 Article 4

2003

Striking the Balance: National Security vs. Civil Liberties

Robert N. Davis

STRIKING THE BALANCE: NATIONAL SECURITY VS. CIVIL LIBERTIES

Robert N. Davis[*]

I. INTRODUCTION

American national security law has come full circle. Between 1945 and 1978, the intelligence community and the executive branch used the national security legal structure to monitor organizations and intrude on the civil liberties of American citizens.[1] Critics argued that the executive branch abused its intelligence collection power during the Cold War in the name of national security.[2] The Foreign Intelligence Surveillance Act ("FISA")[3] was passed in 1978 after findings that intelligence agencies had abused the privacy rights of Americans.[4] FISA was an attempt to provide greater protection of civil liberties by erecting a wall between intelligence collection and law enforcement.[5] Civil liberties organizations now argue, however, that the wall is being eroded by the passage of the Uniting and Strengthening America by Providing Appropriate

* Professor of Law, Stetson University College of Law. Professor Davis teaches international security law and policy, is a member of the ABA Standing Committee on Law and National Security and is an active member in the United States Navy Reserves. Professor Davis would like to acknowledge the excellent research assistance of third-year law student, Sarah Stork.

1. SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK THREE, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP. NO. 94–755, at 740 (9th Cong. 2nd Sess. 1976), The Assassination Archives and Research Center, a*vailable at* http://www.aarclibrary.org/publib/church/contents.htm [hereinafter Church Report Book Three].

2. *Before the United States Senate Judiciary Committee, Subcommittee on the Constitution, Federalism, and Property Rights,* 107th Cong. (Oct. 3, 2001) (testimony of Dr. Morton H. Halperin, Senior Fellow, The Council on Foreign Relations and Chair, Advisory Board, Center for National Security Studies), Center for Democracy and Technology, *available at* http://www.cdt.org/security/011003halperin.pdf [hereinafter Halperin Statement].

3. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C. (1994)).

4. Halperin Statement, *supra* note 2, at 1.

5. Halperin Statement, *supra* note 2, at 2.

Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act").[6]

The USA Patriot Act was passed in the wake of the terrorist attacks of September 11, 2001.[7] Deliberations over the USA Patriot Act included five weeks of intense, round-the-clock negotiations by members of Congress, and congressional oversight committees.[8] The House vote on the Act was three hundred fifty-six for and sixty-six against, and the Senate vote was ninety-eight for and one against.[9] The Act was signed into law on October 26, 2001, over a month after the terrorist attack.[10] The USA Patriot Act was adopted as an effort to strengthen national security but some believe it overreaches by sacrificing civil liberties for the benefit of national security.[11]

The passage of FISA was a reaction to executive branch abuses of civil liberties[12] which were made possible by the non-regulation of surveillance for national security purposes.[13] During this period, the executive branch spied on organized crime

6. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (to be codified at 50 U.S.C. § 401(a)). This Act was passed in response to the attacks of September 11, 2001.

7. *See generally* Charles Doyle, The USA Patriot Act: A Sketch, Congressional Research Service Report for Congress, *at* http://www.fas.org/irp/crs/RS21203.pdf (last visited Oct. 6, 2003).

8. The Center for National Security Studies, USA Patriot Act, *at* http://cnss.gwu.edu/~cnss/patriotact.htm (last visited Oct. 17, 2003). *See* Robert O'Harrow Jr., *Six Weeks in Autumn*, WASH. POST, Oct. 27, 2002, *available at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A1999-2002Oct22&notFound=true.

9. Leon, *Citizens Blast Patriot Act*, *supra* note 9. *See also* Electronic Frontier Foundation, EFF Analysis of the Provisions of the USA Patriot Act, *at* http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.html (last visited Oct. 17, 2003).

10. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (to be codified at 50 U.S.C. § 401 (a)).

11. Michael Leon, *Citizens Blast Patriot Act Madison Passes Civil Liberties Resolution*, Counter Punch, *at* http://www.counterpunch.org/leon1016.html (last visited Oct. 17, 2003).

12. Halperin Statement, *supra* note 2, at 1.

13. *See* Olmstead v. United States, 277 U.S. 438 (1928); *see generally* Gregory E. Birkenstock, *The Foreign Intelligence Surveillance Act and Standards of Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 846–47 (Feb. 1992) [hereinafter Birkenstock].

figures, citizens suspected of having communist ties, and Americans who led radical causes.[14] The terrorist attacks of September 11, 2001 led to a flurry of legislative activity, attempting to enhance national security.[15] The legislation enacted to enhance the structure of the nation's security provisions included, *inter alia*, the Aviation and Transportation Security Act,[16] and the Homeland Defense Department Act.[17] The USA Patriot Act, initiated by Attorney General John Ashcroft, amended over 15 federal statutes.[18] The Attorney General has recently spent time defending the USA Patriot Act against those who argue that civil liberties are at risk because the Act's provisions have provided such expansive law enforcement powers to the executive branch.[19] These critics argue that the USA Patriot Act encroaches on the privacy rights of Americans in the name of national security by allowing law enforcement to conduct intrusive surveillance of emails, telephone conversations, business and library records, and computer use.[20]

The political climate at the time FISA was adopted was very much like the political climate surrounding the passage of the USA Patriot Act in that the safety of the nation and the constitutional rights of citizens were in conflict. However, it is possible for national security legislation to protect civil liberties, while achieving its national security objectives. In theory, the balance must be struck in a manner that preserves the peace and security of the nation while at the same time preserving the constitutional rights and civil liberties of all Americans. In order to achieve the appropriate balance between national secu-

14. Birkenstock, *supra* note 13, at 847–49.

15. Electronic Privacy Information Center, The USA Patriot Act, *at* http://www.epic.org/privacy/terrorism/usapatriot (last visited Sept. 15, 2003) [hereinafter Electronic Privacy Information Center, The USA Patriot Act].

16. Aviation Transportation Safety and System Stabilization Act, Pub.L. 107–42, 115 Stat. 230, (codified at 50 U.S.C.A. § 40101 (West 2001)).

17. Homeland Defense Department Act, 6 U.S.C.A. § 111 (West 2002).

18. American Library Association, The USA Patriot Act in the Library, *at* http://www.ala.org/alaorg/oif/usapatriotlibrary.html (last visited July 19, 2002).

19. Kevin Johnson & Toni Locy, *Patriot Act at Heart of Ashcroft's Influence*, USA TODAY, Sept. 16, 2003, at 8A.

20. David Cole, *On the Road with Ashcroft: He's Trying to Talk Up the Patriot Act, but Americans May No Longer be Buying*, THE NATION, Sept. 22, 2003, at 22.

rity and civil liberties, creative legislative and security initiatives must be pursued and anyone who abuses these new measures, including individual law enforcement officers or the executive branch itself, must be held accountable.

National security and civil liberty interests are not mutually exclusive. We can and must balance both interests appropriately because, in the final analysis, if we cannot secure our nation, civil liberties will mean very little.

History demonstrates that when the nation is *in extremis*, laws bend. Several examples prove this point. President Lincoln ordered a blockade of the southern ports and suspended the right of *habeas corpus* during the Civil War.[21] During World War II, the U.S. ordered the internment of Japanese Americans on the West Coast.[22] Most recently, during the war on terrorism, several American citizens were indefinitely detained by the military as "enemy combatants."[23] Precedent supports the government. During World War II, the federal courts upheld the government's right to hold captured Nazi spies as unlawful enemy combatants.[24] The Latin maxim, *inter arma silent leges* is often invoked to explain the government's tendency toward self-preservation during national emergency. The phrase means "in times of war, the laws are silent."[25] Yet, the laws are not silent, nor should they be. The laws will probably be interpreted to support the government's tendency toward self-preservation when a "threat to the nation's security is real," but they should never be silent altogether.[26]

The USA Patriot Act is not perfect; no piece of legislation is. However, it is an effort to fix our structure in a way that is intended to make us all safe. The Act contains sunset provisions and will probably need future amendment.[27] The USA Patriot

21. *See Ex parte* Milligan, 71 U.S. 2 (1866); *see generally* WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME (1998).

22. *See generally* Korematsu v. United States, 324 U.S. 885 (1945).

23. Ruth Wedgwood, *Lawyers at War*, WALL ST. J., Feb. 18, 2003 at A22.

24. *Ex parte* Quirin v. Cox, 317 U.S. 1, 26 (1942).

25. David G. Savage, *Laws Bend in Time of War, Rehnquist Says*, L.A. TIMES, June 15, 2002, at A22.

26. *Id*.

27. Currently, work is being done to amend the USA Patriot Act. *See* Electronic Frontier Foundation, Draft USA Patriot Act II, *at* http://www.eff.org/Censorship/Terrorism_militias/patriot2draft.html (last visited Feb. 10, 2003) [hereinafter Draft USA Patriot Act II].

Act is not the answer to terrorism–it is only one of the tools that we will use to prosecute the global war against terrorism. It is in the process of winning that war that we will protect the freedoms that we all cherish.

This Article will begin with a history of U.S. intelligence gathering. It will discuss four of the key documents that created the National Security Agency ("NSA") and provide for its intelligence gathering authority. These key documents are The National Security Act of 1947 ("The National Security Act"),[28] the "Truman Memorandum,"[29] Executive Order 12,333[30] and FISA.

This Article will then discuss the impact of national security legislation on Fourth Amendment Rights by surveying litigation under FISA, and will also discuss the anticipated effects of the USA Patriot Act.[31] It will compare the history of FISA and the circumstances surrounding its passage with the circumstances leading to the adoption of the USA Patriot Act and will analyze the two Acts' impact on intelligence collection and information sharing with law enforcement agencies.

This Article will conclude by suggesting that the appropriate balance between civil liberties and national security is achieved only when a nation is free from internal and external threats. However, the nation's security ultimately must be a priority, and a condition precedent toward securing civil liberties. When the nation is secure, its people are secure and when a nation is under attack, civil liberties become secondary to national security.

---

28. *See generally* The National Security Act of 1947, 50 U.S.C. § 401 *et seq*. (2000).

29. Memorandum from Harry S. Truman to Secretaries of State and Defense (Oct. 24, 1952), The National Security Agency, *available at* http://www.nsa.gov/docs/efoia/released/truman.truman.tif [hereinafter Truman Memorandum].

30. *See generally* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

31. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (to be codified at 50 U.S.C. § 401(a)).

II. THE HISTORY OF INTELLIGENCE GATHERING

A. The National Security Act of 1947

After the conclusion of World War II, the President and Congress reorganized the U.S. defense establishment.[32] The goal of enacting The National Security Act was to provide a comprehensive program for the future security of the U.S.[33]

The National Security Act created the Department of Defense ("DOD") to replace the War Department with the Departments of the Army, Navy and Air Force.[34] Additionally, this Act established the National Security Council ("NSC"),[35] restructured the

---

32. Wikipedia Encyclopedia, National Security Act of 1947, The National Security Act of 1947, *at* http://www.wikipedia.org/wiki/National_ Security_ Act_of_1947 (last visited Oct. 11, 2002).

33. The National Security Act of 1947, 50 U.S.C. § 401 (2000). Section § 401 entitled "Congressional Declaration of Purpose" accompanying the Act provided:

> In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide a Department of Defense, including the three military Departments of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services; to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands; to eliminate unnecessary duplication in the Department of Defense, and particularly in the field of research and engineering by vesting its overall direction and control in the Secretary of Defense; to provide more effective, efficient, and economical administration in the Department of Defense; to provide for the unified strategic direction of the combatant forces, for their operation under unified command, and for their integration into an efficient team of land, naval, and air forces but not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff.

Id.

34. The Foreign Intelligence Surveillance Act, 50 U.S.C. § 401 (1994).

35. *Id.* § 402. The National Security Council was established by the National Security Act of 1947 to advise the President regarding domestic, for-

intelligence community, authorized certain agencies within DOD to provide assistance to law enforcement agencies, and restricted intelligence sharing with the United Nations.[36] The Secretary of Defense was also given responsibility, through the NSA, for the "continued operation of an effective unified organization for the conduct of signals intelligence activities. . . ."[37]

B. The Truman Memorandum of 1954: The Birth of the National Security Agency

The NSA "coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information."[38] It performs electronic surveillance, that is, communications listening or monitoring, to collect foreign intelligence information for the intelligence community, the military and government policymakers.[39] This highly specialized mission protects information systems of the U.S. and produces information about other countries.[40] The NSA works with the intelligence community, to keep decision makers informed and the country secure.[41]

---

eign, and military policies relating to national security. The National Security Council is composed of the President, Vice President, Secretary of State, Secretary of Defense, Director for Mutual Security, Chairman of the National Security Resources Board, the Secretaries and Under Secretaries of other executive departments and of the military departments, the Chairman of the Munitions Board, and the Chairman of the Research and Development Board. *Id.*

36. *Id*. §§ 401–404(g) (2000).

37. *Id*. §§ 403–405 (2000).

38. The National Security Agency, About the National Security Agency, *at* www.nsa.gov/about_nsa.index.html (last visited Oct. 11, 2003) [hereinafter NSA Website].

39. *Hearing Before the House Permanent Select Committee on Intelligence*, 106th Cong. 1 (Apr. 12, 2000) (statement for the Record of NSA Director Lt. Gen. Michael V. Hayden, USAF), *available at* www.nsa.gov/releases/DIR_HPSC1_12Apr.pdf [hereinafter Hayden Statement].

40. *See* NSA Website, *supra* note 38. Just two examples of the kinds of intelligence provided by the NSA is its Signals Intelligence (SIGNIT) and its Information Systems security (INFOSEC) mission. Both of these programs have become increasingly significant.

41. *See* The National Security Agency, NSA and the Intelligence Community, *at* http://www.nsa.gov/about_nsa/nsa_role (last visited Oct. 17, 2003).

Historically, the NSA operated in secrecy.[42] Little was known about its mission or structure and much less about its operating budget.[43] Indeed, one scholar has described the birth of the NSA as shrouded in silence.[44] Much more information about the NSA is now available as a result of provisions contained in Executive Order 12,958,[45] which requires the declassification of all permanently classified documents 25 years or older.[46] As a result of this Executive Order, the NSA began a declassification effort known as Opendoor.[47] At its founding, the perception and reality of the NSA was that it was a unique top secret agency. That perception and reality remain true today, though the NSA is no longer cloaked in the impenetrable layers of secrecy that accompanied its birth.

---

42. JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY 15 (1983) [hereinafter BAMFORD].

43. Staci I. Levin, *Who Are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls*, 30 LAW & POL'Y INT'L BUS. 529, 552 n.17 (1999).

44. *See* BAMFORD, *supra* note 42, at 1. James Bamford describes the birth of the NSA in the following manner:

> At 12:01 on the morning of November 4, 1952, a new federal agency was born. Unlike other such bureaucratic births, however, this one arrived in silence. No news coverage, no congressional debate, no press announcement, not even the whisper of a rumor. Nor could any mention of the new organization be found in *The Government Organization Manual* or the *Federal Register* or the Congressional Record. Equally invisible were the new agency's director, its numerous buildings, and its ten thousand employees. Eleven days earlier, on October 24, President Harry S. Truman scratched his signature on the bottom of a seven-page presidential memorandum addressed to secretary of State Dean G. Acheson and Secretary of Defense Robert A. Lovett. Classified top secret and stamped with a code word that was itself classified, the order directed the establishment of an agency to be known as the National Security Agency. It was the birth certificate for America's newest and most secret agency, so secret in fact that only a handful in the government would be permitted to know of its existence. Even the date set for its birth was most likely designed for maximum secrecy: should any hint of its creation leak out, it would surely be swallowed up in the other news of the day—the presidential election of 1952.

Id.

45. Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 20, 1995).

46. *Id*. at 19,832.

47. *See* The National Security Agency, What's in the Database, OpenDoor, *at* www.nsa.gov/programs/opendoor/scope.html (last visited Sept. 29, 2003).

The NSA was not established by a statute, but rather by a presidential memorandum ("The Truman Memorandum") addressed to the Secretary of State and Secretary of Defense regarding communications intelligence activities.[48] In his memorandum, President Truman recognized that "communications intelligence ("COMINT") activities of the U.S. are a national responsibility."[49] It further provides that the NSA's mission "shall be to provide an effective, unified organization and control of the communications intelligence activities of the U.S. conducted against foreign governments, to provide for integrated operational policies and procedures pertaining thereto."[50] Pursuant to the memorandum, the NSA, in performing its COMINT mission, "stands outside the framework of other general intelligence activities."[51] It is this description of the NSA's COMINT activities that helped create the perception that the NSA was once shielded from scrutiny and that enabled the NSA to claim that it had a unique mission. Thus, historically the NSA maintained that "no existing statutes control, limit, or define the signals intelligence activities of NSA."[52] The NSA's General Counsel also asserted that the Fourth Amendment of the United States Constitution did not apply to the NSA when

48. BAMFORD, *supra* note 42, at 1. *See also* LAWS AFFECTING THE NATIONAL SECURITY AGENCY, OFFICE OF THE GENERAL COUNSEL Section III-9 (1998).

49. BAMFORD, *supra* note 42, at 1.

50. *Id*.

51. Truman Memorandum, *supra* note 29. The Truman Memorandum provides:

> The special nature of COMINT activities requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Orders, directives, policies, or recommendations of any authority of the Executive Branch relating to the collection, production, security, handling, dissemination, or utilization of intelligence, and/or classified material, shall not be applicable to COMINT activities, unless specifically so stated and issued by competent departmental or agency authority represented on the Board. Other National Security Council Intelligence Directive to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to COMINT activities, unless the National Security Council has made its directive specifically applicable to COMINT.

Id.

52. Church Report Book Three, *supra* note 1, at 736.

it intercepted international communications by American citizens.[53]

In 1976 Congress established a Committee to begin investigating the NSA for possible abuse of authority.[54] The Committee, led by Senator Frank Church, produced a final report that suggested that the NSA had violated the Constitutional rights of Americans.[55] The Committee pointed to the use of watch lists and the interception of other communications as evidence of the NSA abusing its authority.[56] It further uncovered that the NSA had intercepted millions of telegraphs and messages over the course of thirty years.[57] Two surveillance programs which were cited by the Committee were Operation Shamrock and Operation Minaret.[58] Operation Shamrock was described by the Church Committee report in the following manner:

> From August 1945 until May 1975, NSA received copies of millions of international telegrams sent to, from, or transiting the United States. Codenamed Operation Shamrock, this was the largest governmental interception program affecting Americans, dwarfing CIA's mail opening program by comparison. Of the messages provided to NSA by the three major international telegraph companies, it is estimated that in later years approximately 150,000 per month were reviewed by NSA analysts. NSA states that the original purpose of the program was to obtain the enciphered telegrams of certain foreign targets. Nevertheless, NSA had access to virtually all the international telegrams of Americans carried by RCA Global and ITT World Communications (footnote omitted). Once obtained, these telegrams were available for analysis and dissemination according to NSA's selection criteria, which included the watch lists.[59]

53. *Id*.

54. INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK TWO, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP. NO. 94–755 (9th Cong. 2nd Sess. 1976), *available at* http://www.aarclibrary.org/publib/church/contents.htm [hereinafter Church Report Book Two].

55. David Ruppe, *Big Brother is Listening*, ABCNews.com, (Dec. 17, 2000), *available at* www.abcnews.go.com/sections/world/dailynews/spyII_990727.html [hereinafter Ruppe]; Church Report Book Three, *supra* note 1, at 31.

56. Church Report Book Three, *supra* note 1, at 739.

57. *Id.* at 740.

58. *Id.* at 739–40.

59. *Id*. at 740.

Project Minaret was the codename given to the watch list program.[60] The Church Committee report described Project Minaret in the following manner:

> From the early 1960s until 1973, NSA intercepted and disseminated international communications of selected American citizens and groups on the basis of lists of names supplied by other Government agencies. In 1967, as part of a general concern within the intelligence community over civil disturbances and peace demonstrations, NSA responded to Defense Department requests by expanding its watch list program. Watch lists came to include the names of individuals, groups, and organizations involved in domestic antiwar and civil rights activities in an attempt to discover if there was "foreign influence" on them (footnote omitted).
>
> In 1969, NSA formalized the watch list program under the codename Minaret. The program applied not only to alleged foreign influence on domestic dissent, but also to American groups and individuals whose activities "may result in civil disturbances or otherwise subvert the national security of the U.S." (footnote omitted) At the same time, NSA instructed its personnel to "restrict the knowledge" that NSA was collecting such information and to keep its name off the disseminated "product."[61]

These activities, among others, created concerns that the NSA was routinely invading the privacy of American citizens.[62] Privacy concerns resulted in new legislation affecting U.S. intelligence agencies that constrained domestic surveillance activities.[63] Executive Order 12,333[64] and FISA[65] were two such attempts to reign in some of the NSA's questionable tactics.

---

60. *Id*. at 739.

61. *Id.* at 739. In August 1973, NSA's new director, General Lew Allen, Jr., suspended the dissemination of messages under the program pending recertification of agency requirements. *Id*.

62. *See* Ruppe, *supra* note 55.

63. *Id*. Congressional Hearings in the 1970s "revealed the NSA had been engaging in serious abuses of U.S. citizens' Fourth Amendment rights. . . . Following the hearings, Congress in 1978 passed the Foreign Intelligence Surveillance Act, restricting to a large extent the spy agency's ability to collect information on Americans." *Id*.

C. Executive Order 12,333

Executive Order 12,333[66] was issued by President Reagan on December 4, 1981.[67] The preamble for Executive Order 12,333 provides that intelligence collection is essential to the national security of the U.S.[68] Pursuant to the order, the NSA is authorized to collect, process and disseminate SIGINT information for national foreign intelligence and counterintelligence purposes to support U.S. military operations.[69] No other government agency is authorized to engage in signals intelligence activities unless authorized by the Secretary of Defense.[70] The NSA, however, is only authorized to collect electronic communications for foreign intelligence purposes and may only disseminate this information to authorized government recipients.[71]

Part 1 of Executive Order 12,333, titled Goals, Direction, Duties, and Responsibilities with Respect to the National Intelligence Effort,[72] requires that the U.S. intelligence effort provide the President and the NSC information to protect the U.S. against national security threats and to conduct and develop foreign defense and economic policy.[73] Part I only authorizes collection that is consistent with the law and mindful of the constitutional rights of United States persons.[74]

Part 2, Conduct of Intelligence Activities, strives to achieve a "balance between the acquisition of essential information and protection of individual interests,"[75] by providing that such collection "will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and appli-

64. Exec. Order No. 12,333, 3 C.F.R. 200, 210, 212 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

65. The Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1862 (1994).

66. Exec. Order No. 12,333, 3 C.F.R. 200, 210, 216 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

67. *Id*. at 200.

68. *Id.*

69. *Id.* at 208.

70. *Id.*

71. *Id.*

72. *Id.* at 201.

73. *Id.*

74. *Id*. at 208.

75. *Id*. at 210.

cable law and respectful of the principles upon which the U.S. was founded."[76]

Executive Order 12,333 is intended to "enhance human and technical collection techniques, especially those undertaken abroad…"[77] in order to acquire foreign intelligence and to counter international terrorism and espionage conducted by foreign powers.[78] Section 2.3, Collection of Information, specifically limits the ability to perform intelligence collection on United States persons.[79] It specifies the types of information that could be the subject of collection efforts. For example, information may be collected on a U.S. person only with the consent of the person involved.[80] Commercial information that constitutes foreign intelligence or counterintelligence may be collected.[81] Collection efforts may also include information needed to protect the safety of people or organizations, sources or methods, and incidentally obtained information that indicates a violation of law.[82]

Collection efforts by intelligence agencies are restricted by Section 2.4, Collection Techniques, which requires "use [of the] least intrusive collection techniques feasible within the U.S. or

76. *Id*.

77. *Id.* at 210.

78. *Id.* Pursuant to Section 2.5, to carry out this mission, intelligence agencies must be authorized by the Attorney General to conduct warrantless physical searches of property to obtain foreign intelligence and counterintelligence information. Pursuant to Section 3.4(d), foreign intelligence is defined as: "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities." Section 3.4(a) defines counterintelligence as: "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs." *Id*.

79. Exec. Order No. 12,333, 3 C.F.R. 200, 211 (1982), *reprinted in* 50 U.S.C. § 401 (2000). Section 2.3 provides that: "Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order." *Id*.

80. *Id*. at 211.

81. *Id*.

82. *Id*. at 203, 211.

directed against United States persons abroad."[83] Section 2.4 specifically forbids the Central Intelligence Agency ("CIA") to conduct electronic surveillance within the U.S., unconsented physical searches in the U.S. by agencies other than the Federal Bureau of Investigation ("FBI"), and physical surveillance of Americans in the U.S.[84] These general proscriptions provide exceptions for limited purposes.[85]

Section 2.5 requires the Attorney General's approval before collection efforts can be directed "within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes."[86] In such a case, the Attorney General must determine in each case that there is probable cause to believe that the technique is directed against a foreign power or its agent.[87] The NSA must convince the Attorney General that the person is an agent of a foreign power, a spy, a terrorist, a saboteur or someone who will provide assistance to such individuals or organizations.[88]

---

83. *Id*. at 212.

84. *Id*.

85. *Id*. The exception is that the CIA may not engage in domestic electronic surveillance generally, however, it may do so for the purposes of training, testing, or conducting countermeasures to foreign surveillance.

86. *Id.*

87. *Id.*

88. *Id*. at 214. Lt. Gen. Michael Hayden described the NSA's intelligence collection efforts as follows:

> NSA's collection of foreign intelligence from foreign individuals and entities is designed to minimize the incidental, or unintentional, collection of communications to, from, or about U.S. persons. When NSA does acquire information about a U.S. person, NSA's reporting does not disclose that person's identity, and NSA will only do so upon a specific request that meets the standard derived from statute and imposed by Executive Order regulation…that is, the information is necessary to understand a particular piece of foreign intelligence or assess its importance. Similarly, no identities of U.S. persons may be disseminated (that is, transmitted to another Government department or agency) by NSA unless doing so is necessary to understand a particular piece of foreign intelligence or assess its importance. For example, if NSA intercepted a communication indicating that a terrorist was about to harm a U.S. person, the name of the U.S. person would be retained and disseminated to appropriate law enforcement officials.

Hayden Statement, *supra* note 39, at 6.

Another significant feature of Executive Order 12,333 is the legislative oversight it creates.[89] Section 3.1, Congressional Oversight, requires the intelligence agencies to "cooperate with …Congress in the conduct of its responsibilities for oversight of intelligence activities."[90] Judicial oversight is also a part of Executive Order 12,333.[91] Section 2.5 references FISA which requires the Foreign Intelligence Surveillance Court to issue court orders for electronic surveillance directed against foreign powers or their agents.[92]

Executive Order 11,905,[93] issued by President Ford in 1976, and Executive Order 12,036,[94] issued by President Carter in 1978, further limited intelligence gathering methods.[95] Both prohibited the intelligence agencies from conducting warrantless domestic physical searches unless appropriate executive branch approval was obtained.[96]

Thus, Executive Orders 12,333, 11,905 and 12,036 contained a common thread. They were all intended to stop the earlier abuses by intelligence agencies. To that end, these executive orders limited intelligence gathering methods, restricted collection efforts, required attorney general approval and provided for legislative oversight.

D. Key Provisions of FISA

FISA was passed by the 95th Congress in 1978 and signed into law by President Carter.[97] FISA was the product of compromises between the executive and legislative branches in

89. Exec. Order No. 12,333, 3 C.F.R. 200, 214 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

90. *Id*.

91. *Id*. at 212.

92. The Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1804–1805 (1994).

93. *See generally* Exec. Order No. 11,905, 3 C.F.R. 90, 99 (1976), *reprinted in* 50 U.S.C.§ 401 (Supp. I 1977).

94. Exec. Order No. 12,036, 3 C.F.R. 112, 126–28 (1979), *reprinted in* 50 U.S.C. § 401 (Supp. IV 1980).

95. *See generally* Exec. Order No. 11,905, 3 C.F.R. 90, 99 (1976), *reprinted in* 50 U.S.C. § 401 (Supp. I 1977) and Exec. Order No. 12,036, 3 C.F.R. 112, 126–28 (1979), *reprinted in* 50 U.S.C. § 401 (Supp. IV 1980).

96. *Id.*

97. Foreign Intelligence Surveillance Act, Pub. L. No. 95–511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

their effort to address abuses in the intelligence agencies revealed by the Church Committee Investigation.[98] FISA was also an attempt to balance the claimed inherent national security authority of the executive branch with the Fourth Amendment's prohibition on unreasonable searches and seizures.[99] The NSA's administrative and legal process for conducting electronic surveillance is largely governed by Executive Order 12,333[100] and FISA.

FISA is a complex statute that has been criticized for lacking "due process and accountability."[101] FISA provides the procedures for obtaining electronic surveillance authorization without a court order.[102] Section 1802 authorizes the President, through the Attorney General, to permit electronic surveillance to acquire foreign intelligence information for a period of up to one year without a court order.[103] The Attorney General must certify that (1) the electronic surveillance is "solely directed" at communications "between or among foreign powers;"[104] (2) there is no "substantial likelihood" that the surveillance will involve a U.S. person;[105] and, (3) that minimization procedures are in effect.[106] Fourth Amendment challenges to this provision have

98. *See generally* Church Report Book Three, *supra* note 1, at 31.

99. U.S. CONST. amend. IV. This amendment 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.

Id. *See also In re* Kevork, 788 F.2d 566, 569 (9th Cir. 1986) (citing, S. REP. NO. 604 and holding that the purpose of FISA was to strike a balance between the need for surveillance and the protection of civil liberties).

100. *See supra* Part II.C.

101. Gerald H. Robinson, *We're Listening! Electronic Eavesdropping, FISA, and the Secret Court*, 36 WILLAMETTE L. REV. 51, 72 (2000) [hereinafter Robinson].

102. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1802 (1994).

103. *Id*. § 1802(a)(1).

104. *Id*. § 1802(a)(1)(A)(i).

105. *Id*. § 1802(a)(1)(B).

106. *Id*. § 1802(a)(1)(C). Under Section 1801(h)

> (b) "Minimization procedures" with respect to electronic surveillance, means

been unsuccessful.[107] In *United States v. Pelton*,[108] the United States Court of Appeals for the Fourth Circuit held that FISA did not violate the Fourth Amendment because the statutory safeguards provided "sufficient protection" of individual rights when balanced against the government's interest in gathering foreign intelligence which is of "paramount importance to national security."[109]

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Id.

107. Robinson, *supra* note 101, at 67.

108. United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), *cert denied*, 486 U.S. 1010 (1988).

109. *Id*. at 1074–75. *See also* United States v. Megahey, 553 F. Supp. 1180, 1192 (E.D.N.Y. 1982) (holding that electronic surveillance of home phone number does not violate Fifth Amendment rights provided object of surveillance is foreign intelligence, even if criminal prosecution may follow). *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) (holding that FISA

FISA also created the Foreign Intelligence Surveillance Court ("FISA Court"),[110] frequently referred to as the "secret court" because it conducts proceedings under specified security rules in a secure room in the Department of Justice ("DOJ").[111] The FISA Court is comprised of seven district court judges designated by the Chief Justice of the United States Supreme Court.[112] The FISA Court's jurisdiction includes hearing applications for and issuing orders approving or denying electronic surveillance within the U.S.[113] Section 1803 also establishes a Court of Review ("FISA Review Court") consisting of three district court or appellate court judges also designated by the Chief Justice.[114] The FISA Review Court has jurisdiction to review the denial of surveillance applications.[115] FISA Court proceedings are required to be conducted expeditiously and the record of the proceedings "shall be maintained under security measures established by the Chief Justice[,] in consultation with the Attorney General, and the Director of Central Intelligence."[116]

Requirements for applications for electronic surveillance orders are detailed in Section 1804.[117] These requirements include, *inter alia*, disclosure of the identity of the federal officer submitting the request and a "statement of the facts and circumstances relied upon by the applicant to justify his belief that — the target of the electronic surveillance is a foreign power or an agent of a foreign power."[118] This section also requires the federal officer to provide a description of the information sought, a statement of the proposed minimization procedures, a

---

evidence may be used in subsequent criminal prosecution but "investigation of the criminal activity cannot be the primary purpose of the surveillance").

110. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1803 (1994).

111. *See* Robinson, *supra* note 101, at 51.

112. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1803(a) (1994).

113. *Id.*

114. *Id.* § 1803(b).

115. *Id*.

116. *Id.* § 1803(c).

117. *Id.* § 1804.

118. *Id*. § 1804(a)(1)-(4). *See* United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000), (citing United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (requiring a statement of reasons to believe that the target of the surveillance is a foreign power or agent of a foreign power, and certification by an executive branch official that the information sought is foreign intelligence information and cannot be obtained by other means). *Id.*

statement of facts concerning previous applications made involving the same people, facilities or places, and a statement of the time period for which the electronic surveillance will be maintained.[119]

Particular findings are required before the FISA Court can issue a surveillance order.[120] Necessary findings include facts submitted by the applicant that there is probable cause to believe the target is a foreign power or agent of a foreign power.[121] In addition, minimization procedures must meet the requirements of the definition found in Section 1804(h).[122] In determining whether probable cause exists to issue a surveillance order, judges may also consider past, current and future activities of the target.[123] Section 1805 requires that an order approving electronic surveillance identify the target, describe the location of each facility, describe the type of information sought, indicate whether physical entry will be used, and the period of time of the electronic surveillance.[124] It also requires that minimization procedures be followed and the applicant compensate the carrier, landlord, or other person furnishing aid to the surveillance effort.[125] The duration of a surveillance order is for a period "necessary to achieve its purpose, or ninety days, whichever is less."[126] However, electronic surveillance against a foreign power target may be for up to one year.[127] An order may be extended on the same basis as the original order upon a new application and new findings.[128]

In *U.S. v. Squillacote*,[129] the United States Court of Appeals for the Fourth Circuit held that where the target of electronic

119. Foreign Intelligence Surveillance Act, 50 U.S.C. §1804(a)(5), (6), (9), (10) (1994).

120. *Id.* § 1805(b).

121. *Id.* § 1805(a)(3)(A). ("No United States person may be considered an agent of a foreign power solely based on the exercise of activities protected under the First Amendment of the United States Constitution….").

122. *Id*. § 1805(a)(4).

123. Foreign Intelligence Surveillance Act, 50 U.S.C.A. § 1805(b) (West 2003) (*amending* 50 U.S.C. § 1805 (1994).

124. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805(b)(1) (1994).

125. *Id* § 1805(b)(2)(A),(D).

126. *Id*. § 1805(d)(1).

127. *Id*.

128. *Id.* § 1805(d)(2).

129. United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000).

surveillance is a "United States person"[130] as defined by FISA, surveillance may be authorized "only if the FISA judge concludes that there is 'probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power, that proposed minimization procedures are sufficient, [and] that the certifications required have been made…'"[131] However, the United States Court of Appeals for the District of Columbia has held that nonresident aliens who are in the U.S. on visitor or student visas do not qualify as "United States persons" under FISA.[132]

FISA restricts the use of information acquired from electronic surveillance concerning any United States person.[133] Acquired information may only be used and disclosed by federal employees without the consent of the United States person when minimization procedures are adhered to.[134] No privileged information acquired will lose its privileged status.[135] Additionally, federal officers may use acquired information only for lawful purposes.[136] If the government intends to use information acquired by electronic surveillance in any proceeding, it must so notify the affected person and the court prior to trial or hearing that it intends to disclose such information.[137] "Any person against whom evidence is obtained or derived from an electronic surveillance…may move to suppress the evidence obtained or derived…on the grounds that…it was unlawfully acquired; or

130. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(i) (1994) defines "United States person" as:

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of the Title 8(1), 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.

131. *Squillacote,* 221 F.3d at 553.

132. ACLU Foundation of Southern California v. Barr, 952 F.2d 457, 464 (D.C. Cir. 1991).

133. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806(a) (1994).

134. *Id.*

135. *Id*.

136. *Id*.

137. *Id*. § 1806(c).

the surveillance was not made in conformity with an order of authorization or approval."[138] The district court, upon notice by the government or an aggrieved individual, will conduct an *in camera* and *ex parte* review of the application, and order any other material relating to the surveillance to determine whether the surveillance was lawfully authorized and conducted.[139] If the surveillance was not lawfully authorized and conducted the district court must suppress the evidence obtained.[140] "If the Court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion" to suppress unless due process requires discovery and disclosure.[141] In *U.S. v. Hamide*, the United States Court of Appeals for the Ninth Circuit held that *in camera* and *ex parte* review under FISA was adequate to ensure that a factual record was sufficiently developed to allow eventual appellate review.[142]

Finally, FISA requires the Attorney General to file a report to the Administrative Office of the United States Court and Congress regarding the number of applications for electronic surveillance orders and extensions approved, modified or denied.[143] The Attorney General is also required to "fully inform" the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence on a semiannual basis, concerning all electronic surveillance.[144] FISA imposes criminal sanctions for intentional violations of electronic surveillance procedures[145] and creates a cause of action for damages for certain individuals[146] who have been subjected to electronic surveillance or about whom such information has been disclosed.[147]

---

138. *Id.* § 1806(e).
139. *Id.* § 1806(f).
140. *Id*. § 1806(g).
141. *Id*.
142. United States v. Hamide, 914 F.2d 1147, 1152 (9th Cir. 1990).
143. The Foreign Intelligence Surveillance Act, 50 U.S.C §1807 (1994).
144. *Id.* § 1808.
145. *Id.* § 1809. This section makes intentional violation a crime punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both. *Id*.
146. Excluding foreign powers or agents of a foreign power. 50 U.S.C. § 1810 (1994).
147. *Id*. § 1810. This section creates a cause of action against any person who committed the violation for actual damages, punitive damages, reasonable attorney's fees and other costs reasonably incurred.

III. THE IMPACT OF NATIONAL SECURITY LEGISLATION ON 4TH AMENDMENT RIGHTS

Before a search warrant can be issued, the Fourth Amendment to the Constitution requires that law enforcement have reasonable grounds to believe that the law is being violated.[148] This requirement helps to limit the focus and targets of criminal investigations, control overzealous law enforcement officers and protect innocent civilians.[149] FISA does not contain this criminal standard of probable cause.[150] Instead, FISA contains a "foreign intelligence standard" of probable cause which requires a showing that the target may be an agent of a foreign government and the place or facility to be searched is being used in furtherance of espionage or terrorist activities.[151] Thus, the criminal standard that requires probable cause for a search warrant and the foreign intelligence standard are very different, in that they require different showings.

A. FISA Jurisprudence

The tension that exists between the need of the executive branch to conduct foreign intelligence surveillance for national security reasons and the right of citizens to be free from unreasonable searches and seizures is due to the difference between executive authority under Article II of the United States Constitution and individual rights under the Fourth Amendment.[152] Electronic surveillance in particular has not been easily categorized in constitutional jurisprudence.[153] As early as *Olmstead v. United States*,[154] a sharply divided Supreme Court had trouble viewing telephone conversations obtained through wiretaps as the equivalent of tangible items subject to seizure.[155] Thus, the

148. *See* Dumbra v. United States, 268 U.S. 435, 441 (1925).

149. *See* Bringer v. United States, 338 U.S. 160, 176 (1949).

150. The Electronic Privacy Information Center, Overview of FISA, *at* http://www.epic.org/privacy/terrorism/fisa (last visited Oct. 4, 2003).

151. *Id*.

152. U.S. CONST. art. II; U.S. CONST. amend. IV.

153. *See* Olmstead v. United States, 277 U.S. 438, 458–66 (1928) (reviewing the "chief cases" where the Supreme Court has confronted and addressed similar Fourth Amendment claims as well as common law rules).

154. *Id.*

155. *Id*. at 466.

telephone conversation in *Olmstead* was admissible in a criminal trial and not subject to the Fourth Amendment's unreasonable search and seizure prohibition.[156] This decision served to encourage the executive branch's use of electronic surveillance.[157] The Federal Communications Act of 1934 ("FCA")[158] and the Supreme Court's decision in *Nardone v. United States*,[159] interpreting the FCA, sought to restrain the use of electronic surveillance.[160] World War II, however, elevated the importance of electronic surveillance and the executive branch's use of electronic surveillance did not wane with the end of the war.[161]

The Supreme Court overruled *Olmstead*, in *Katz v. United St*ates,[162] and introduced the concept of individual privacy expectations.[163] In *Katz,* the court discussed the importance of surveillance activities linked to national security interests, and thus set the stage for FISA.[164] After the *Katz* decision, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968.[165] This Act established procedures for obtaining a warrant and expressly indicated that it was not intended to interfere with the executive authority of the President.[166] By now, the

> Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure. We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

Id.

156. *Id*.

157. *See* Americo R. Cinquegrana, *The Walls (And Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 796 (1989) [hereinafter Cinquegrana].

158. The Federal Communication Act of 1934, 47 U.S.C.A. §§ 151–613 (West 2003).

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

160. Cinquegrana, *supra* note 157, at 797.

161. *Id.* at 798.

162. Katz v. United States, 389 U.S. 347, 353 (1967).

163. Cinquegrana, *supra* note 157, at 800.

164. *Id*.

165. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 211 (codified at 18 U.S.C.A. §§ 2510–2522 (West 2003)).

166. *See* comments to 18 U.S.C.A. § 2510 (West 2003). Under Part 2, entitled "Construction": "In enacting this Chapter, Congress refrained from at-

President claimed inherent powers under Article II to conduct warrantless electronic surveillance for national security purposes.[167] The United States Supreme Court in *United States v. United States District Court for the Eastern District of Michigan*,[168] on facts not involving foreign intelligence surveillance, however, held that the Fourth Amendment required prior judicial approval for domestic electronic surveillance.[169] Thus, the scope of the executive branch's power to conduct warrantless electronic surveillance when acting in the interests of national security remained very much undecided.[170] The lower courts struggled with the issue of the legality of warrantless electronic surveillance for national security purposes.[171] Later Congress, in light of the issues raised by the Church Committee, was more receptive to "the need to regulate electronic surveillance for national security purposes."[172]

In *United States District Court for the Eastern District of Michigan,* the Supreme Court challenged Congress to develop

tempting to convey to the President any power which he did not already possess, and in providing that nothing therein contained should be deemed to limit constitutional powers of the President, Congress did not use language appropriate for grant of power." *Id*.

167. United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 310 (1972).

168. *Id.*

169. *Id*. at 320 (finding a case has not "been made for the requested departure from Fourth Amendment standards"). *Id*.

170. *Id*. at 321–22. (noting the narrow scope of its decision and states "[w]e have not addressed, and express no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents"). *Id.*

171. At the time, five federal courts considered the issue of warrantless electronic surveillance. Of the five, four United States Courts of Appeals were willing to recognize a foreign intelligence exception. *See* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert denied*, 415 U.S. 960 (1974); United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974), *cert denied*, 419 U.S. 881 (1974); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977), *cert denied*, 434 U.S. 890 (1977); and United States v. Truong, 629 F.2d 908, 913 (4th Cir. 1980). In Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) the Court of Appeals for the District of Columbia Circuit was the only court to "cast fundamental doubt" on the constitutional basis for warrantless electronic surveillance. However, this case did not involve a foreign power or agent of a foreign power. Nevertheless, the Court of Appeals expressed its belief that all warrantless electronic surveillance would be unreasonable unless exigencies could justify the constitutional invasion. *Id.*

172. Cinquegrana, *supra* note 157, at 807.

national security standards for electronic surveillance that differed from the law enforcement standards in the Omnibus Crime Control and Safe Streets Act of 1968.[173] Congress and the courts were uncertain regarding the scope of executive branch authority in the area of national security and foreign surveillance.[174] Executive branch practice coupled with ambiguity regarding an appropriate judicial role, if any, in restricting electronic surveillance, required Congress to address issues of separation of powers.[175] The Church Committee's investigation revealed abuses by the intelligence agencies in violation of individual privacy interests.[176] These abuses of executive discretion were attributable to unsettled case law and lack of congressional or judicial standards.[177] As a result of its investigation, the Church Committee recommended that Congress develop legislation to restrict electronic surveillance for intelligence purposes.[178] The Committee suggested that electronic surveillance within the U.S. be restricted to the FBI, pursuant to a judicial warrant.[179]

Congress questioned whether it was appropriate to involve Article III judges in the approval process for electronic surveillance for national security purposes.[180] The Congressional Research Service[181] addressed this concern in a memorandum that concluded that surveillance approval is a case or controversy as that term is used in Article III, and judicial supervision was appropriate in this area because of the government and privacy interests at stake.[182]

---

173. *United States District Court for the Eastern District of Michigan*, 407 U.S. at 322–23.

174. *Id*. at 322.

175. *Id*. at 322–24.

176. Church Report Book Three, *supra* note 1, at 735.

177. *See* Cinquegrana, *supra* note 157, at 807; Church Report Book Two, *supra* note 54, at 186–87.

178. *See generally* Church Report Book Two, *supra* note 54.

179. Church Report Book Two at 297, 299; *see also* Cinquegrana, *supra* note 157, at 807.

180. Cinquegrana, *supra* note 157, at 808 n. 81.

181. The Congressional Research Service serves Congress throughout the legislative process by providing comprehensive and reliable legislative research and analysis.

182. Cinquegrana, *supra* note 157, at 808.

The constitutional issues that were debated before FISA was enacted continue to be the subject of debate.[183] Does Congress have the authority to limit the executive authority in the area of electronic surveillance for foreign/domestic intelligence collection? Is warrantless electronic surveillance for foreign intelligence collection compatible with the Fourth Amendment? Does Article III permit the FISA Court to conduct a hearing *in camera* and *ex parte*?[184] In *United States v. Duggan*,[185] the United States Court of Appeals for the Second Circuit had occasion to examine these constitutional issues and concluded that the procedures in FISA adequately balanced the individual's Fourth Amendment rights with the need to obtain foreign intelligence information.[186]

Before FISA was enacted, courts that addressed the issue of the warrant requirement in the context of national security surveillance concluded that the President had inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information.[187] The prevailing view was that electronic surveillance for foreign intelligence purposes constituted an exception to the Fourth Amendment's warrant require-

183. *Id*. at 816.

184. These constitutional questions are now magnified in light of the events that took place on the morning of September 11, 2001 in New York City and Washington, D.C. In one of the worst terrorist attacks in the history of the civilized world, the twin towers of the World Trade Center in New York were leveled as hijacked commercial airliners were flown into the towers and exploded. The Pentagon also came under attack when another hijacked commercial airliner plowed into it approximately one hour later. *See* Serge Schmemann, *U.S. Attacked; President Vows to Exact Punishment for 'Evil'*, N.Y. TIMES, Sept. 12, 2001, at A1.

185. United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

186. *Id*. at 73. The defendants in *Duggan* were agents of the Provisional Irish Republican Army who sought to acquire explosives, weapons, ammunition, and remote-controlled detonation devices from the United States to be exported to Northern Ireland for use in terrorist activities. The defendants moved to suppress evidence from FISA surveillance. They argued, *inter alia*, that FISA surveillance was so broad that it violated due process, separation of powers, and equal protection to aliens. *Id.*

187. *Id.* at 72. *See* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 419 U.S. 881 (1974); United States v. Butenko, 318 F. Supp. 66 (D.N.J. 1970), *rev'd en banc*, 494 F.2d 593, 604–06 (3rd Cir. 1974), *and cert. denied*, 419 U.S. 881 (1974).

ment.[188] While the Supreme Court declined to address this issue in *United States v. United States District Court for the Eastern District of Michigan,* it made clear that Fourth Amendment warrant requirements may change when different governmental interests, like national security, are at stake.[189]

FISA was again challenged in the 1985 case of *In re Kevork*.[190] In *Kevork,* the Supreme Court of Ontario, Canada "issued an order for a commission to take evidence of eight witnesses in Los Angeles, California."[191] These witnesses had overheard conversations of the defendants pursuant to orders issued by the FISA Court.[192] The purpose of the commission was to gather evidence in a pending criminal prosecution in Canada.[193] A

188. *Duggan*, 743 F.2d at 72. *See* United States v. Buck, 548 F.2d 871 (9th Cir. 1977), *cert. denied*, 434 U.S. 890 (1977).

189. *See* United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 321–22 (1972). The Supreme Court held:

> [W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.
>
> Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens. The warrant application may vary according to the governmental interest to be pursued and the nature of citizen's rights requiring protection.

Id. at 322–23.

190. *In re* Kevork, 634 F. Supp. 1002 (C.D. Cal. 1985).

191. *Id.* at 1004.

192. *Id*. at 1005.

193. *Id*.

United States District Court judge and a justice from the Supreme Court of Ontario were appointed as commissioners to obtain the evidence requested.[194] The information sought involved private communications between some of the defendants regarding a conspiracy to murder a Turkish diplomat which the FBI intercepted.[195] The conversations were overheard through microphones and a telephone tap installed in the home of a non-party.[196] The defendants moved to block the Commission from receiving the testimony and evidence by attacking the constitutionality of FISA.[197] Because the defendants' motion to suppress evidence involved the bona fides of the Commission receiving evidence obtained through an order issued under FISA, a United States District Court judge considered the defendants' motion.[198]

The defendants argued that FISA was unconstitutional and violated the Fourth Amendment because its orders were not search warrants and did not meet probable cause requirements.[199] They also argued that FISA was vague because it "contains no real limits regarding who or what may be a proper surveillance target."[200] The defendants also contended that FISA violated Article III of the Constitution because the FISA Court was not a proper Article III court.[201] Finally they argued that it improperly delegated judicial power to the executive branch.[202]

The court held that FISA did not violate the Fourth Amendment because the Fourth Amendment is flexible and different standards may be applied to meet other governmental interests such as foreign intelligence collection.[203] The court also concluded that the defendants' argument that FISA was vague was without merit, holding that FISA set out reasonable standards which must be met before anyone can become the target of for-

194. *Id*. at 1004.
195. *Id.*
196. *Id*. at 1005.
197. *Id.* at 1010.
198. *See id*. at 1005.
199. *Id*. at 1010.
200. *Id*. at 1012.
201. *Id.* at 1014.
202. *Id*.
203. *See id*. at 1010–11.

eign intelligence surveillance.[204] Regarding the defendants' contention that FISA violated Article III, the court concluded that there was substantial precedent for specialized courts such as the FISA Court.[205]

At the time FISA was debated and passed, Congress was aware of the abuses of domestic national security surveillance and of the legal uncertainty of whether the executive branch had inherent authority to execute warrantless electronic surveillance for foreign intelligence collection.[206] Thus, FISA was passed in order "to settle the unresolved question of the applicability of the Fourth Amendment warrant requirement to electronic surveillance for foreign intelligence purposes, and to 'remove any doubt as to the lawfulness of such surveillance.'"[207] The court concluded that FISA contained well-defined procedures that permitted a FISA Court judge to authorize electronic

204. *See id*. at 1010–12. The court continued: "As the legislative history makes clear, FISA was enacted to 'reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.'" *Id*.

205. *Id*. at 1014.

206. *Id*. at 1011. The court noted that when electronic surveillance is used for intelligence purposes rather than for detecting crimes, different protections may be applied and still be consistent with the Fourth Amendment. The Court stressed that Congress was aware of this aspect citing *United States v. United States District Court for the Eastern District of Michigan* when it passed FISA. *Id*. *See also* SELECT COMMITTEE ON INTELLIGENCE, S. REP. NO. 95–701, (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973. The Report provided:

> The departures here from conventional Fourth Amendment doctrine have, therefore, been given close scrutiny to ensure that the procedures established in FISA are reasonable in relation to legitimate foreign counterintelligence requirements and the protected rights of individuals. Their reasonableness depends, in part, upon an assessment of the difficulties of investigating activities planned, directed, and supported from abroad by foreign intelligence services and foreign-based terrorist groups. The differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities have been taken into account. Other factors include the international responsibilities of the United States, the duties of the Federal Government to the States in matters involving foreign terrorism, and the need to maintain the secrecy of lawful counterintelligence sources and methods.

Id. at 3983.

207. *In re* Kevork, 634 F. Supp. 1002, 1010 (C.D. Cal. 1985) (citing H.R. REP. NO. 95–1283, Pt. I (95th Cong. 2d Sess. 21 (1978)).

surveillance for foreign intelligence purposes without violating the privacy rights of United States citizens.[208] FISA represents a Congressional effort to provide a constitutional structure to foreign intelligence collection that is consistent with the Fourth Amendment.[209] Though the United States Supreme Court has declined to rule on the constitutionality of FISA, the Act has withstood substantial judicial scrutiny.[210]

B. The 1994 Amendments to FISA and their Application to Physical Searches

While FISA was enacted to provide a clear means of authorizing electronic surveillance activities for national security purposes it was unclear whether or not FISA also applied to physical searches.[211] At the time of its passage in 1978, FISA only addressed procedures applicable to electronic searches not physical searches.[212] It would take almost twenty-years before Congress amended FISA and clarified the procedures applicable for physical searches for foreign intelligence purposes.[213] Shortly after the 1994 amendments were passed, President Clinton signed Executive Order 12,949,[214] which recognized that FISA, as amended, now clearly applied to physical searches.[215] Thus, the debate that had occurred regarding whether FISA was intended to apply to electronic surveillance and physical searches ended with the passage of the 1994 FISA amendments and Executive Order 12,949.[216]

The conduct of physical searches under FISA is governed by Sections 1821-1829.[217] These provisions mirror those applicable to electronic surveillance.[218] Physical search is defined by statute to mean:

---

208. *Id*. at 1010.
209. *See id*. at 1014.
210. Cinquegrana, *supra* note 157, at 820.
211. *Id.* at 821–22.
212. Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1811 (1994).
213. *Id*. §§ 1821–1829.
214. Exec. Order No. 12,949, 3 C.F.R. 321 (1996), *reprinted in* 50 U.S.C. § 1822 (1994). *See also* U.S. v. Nicholson, 955 F. Supp. 588, 591 (E.D. Va. 1997).
215. Exec. Order No. 12,949, 3 C.F.R. 321 (1996), *reprinted in* 50 U.S.C. § 1822 (1994).
216. *Id.*
217. Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1821–1829 (1994).
218. *Id*. §§ 1801–1811.

> any physical intrusion within the United States into premises or property…in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes…but does not include (A) "electronic surveillance"… or the (B) acquisition by the United States Government of foreign intelligence information from…means other than electronic surveillance…[219]

FISA authorizes the President through the Attorney General to approve physical searches without a court order to acquire foreign intelligence information for periods of up to one year.[220] The Attorney General must certify that the physical search is directed at property under the control of a foreign power, that there is no substantial likelihood that the search will involve the premises of a United States person, and that minimization procedures are in place.[221] Compensation must be paid for the use of any facilities or assistance necessary to accomplish the physical search.[222]

The FISA Court has jurisdiction to expeditiously hear applications for and grant orders approving physical searches for the purposes of obtaining foreign intelligence information.[223] The FISA Review Court, established under Section 1803, has jurisdiction to review the denial of any application for physical searches made under FISA.[224] An application for a physical search order must, *inter alia*, (1) be made by a federal officer; (2) describe the target of the search in detail and; (3) identify the property targeted as containing foreign intelligence information that is owned or controlled by a foreign power or agent.[225] If a FISA Court judge decides to issue an order for a physical search, the order must contain findings that there exists probable cause to believe that the target is a foreign power or agent, that the premises is owned, used or possessed by a foreign power and that minimization procedures are in place.[226] In determining probable cause, a FISA Court judge may con-

219. *Id*. § 1821(5).
220. *Id.* § 1822(a)(1).
221. *Id*.
222. *Id*. § 1822(a)(4)(A)–(B).
223. *Id*. § 1822(c), (e).
224. *Id*. § 1822(d).
225. *Id*. § 1823(a)(1), (2), (3).
226. *Id*. § 1824(a).

sider past, current and future activities of the target.[227] Physical search orders approved under Section 1824 are for the time period necessary to achieve its purpose or for forty-five days, whichever is less, and the orders may be extended for up to one year.[228] Emergency orders are authorized under Section 1824(d).[229] Information obtained from a physical search concerning a United States person may be disclosed and used by federal officers without the consent of the United States person only in accordance with required minimization procedures.[230]

If the federal government intends to use information obtained from the physical search in any proceeding, the government must notify the target of the search.[231] The target may then submit a motion to suppress on the grounds that the information was unlawfully acquired or the search was not in compliance with the order.[232] The District Court hearing the matter must conduct an *in camera* and *ex parte* review if the Attorney General argues that disclosure would harm the national security of the U.S.[233] Congressional oversight and criminal and civil sanctions are also applicable to the physical search provisions.[234] FISA authorizes the use of pen registers and trap and trace devices for foreign intelligence collection and international terrorism investigations.[235] FISA also authorizes the FBI to have access to business records related to an investigation and to gather information on foreign intelligence or on international terrorism.[236]

227. *Id*. § 1824(b).
228. *Id*. § 1824(c).
229. *Id*. § 1824(d).
230. *Id.* § 1825(a).
231. *Id*. § 1825(d), (f).
232. *Id.* § 1825(d), (f).
233. *Id*. § 1825(g).
234. *Id*. §§ 1826–1828.
235. Foreign Intelligence Surveillance Act, 50 U.S.C.A. § 1842 (West 2003) (amending scattered sections of 50 U.S.C. (1994)). Pen registers are devices which record or decode electronic impulses which identify numbers transmitted on the telephone line. Trap and trace devices capture incoming impulses and identify the originating number. *Id.*
236. *See id.* § 1862.

The application of FISA to physical searches has been a subject of debate for over ten years.[237] The first constitutional challenge to the physical search provisions of FISA was in *United States v. Nicholson*.[238] In a wide-ranging but very brief opinion dismissing defendant's motion to suppress evidence, the court applied pre-1994 FISA law to FISA as amended, in the context of the new physical search authority.[239]

The defendant, Harold Nicholson, was charged with attempted espionage, espionage, and conspiracy to commit espionage in violation of the Espionage Act.[240] During the investigation that led to the defendant's arrest, his "home, office, car, safe deposit box, and personal effects were subject to electronic surveillance and physical searches conducted under FISA."[241] The defendant sought the suppression of the evidence obtained from the electronic surveillance and physical searches contending, *inter alia*, that FISA procedures violate due process, equal protection, separation of powers, the political question doctrine, and the Fourth Amendment.[242]

The issue in *United States v. Nicholson* was whether the 1994 FISA amendments permitting physical searches for foreign intelligence collection were constitutional.[243] The defendant argued that physical searches were more intrusive than electronic searches and must be reviewed under a more stringent constitutional standard than that applied to electronic surveillance.[244] The United States District Court for the Eastern District of Virginia held, that consistent with prior precedent, "...Fourth

237. *See* William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 155–56 (1985) [hereinafter Brown & Cinquegrana].

238. United States v. Nicholson, 955 F. Supp. 588 (E.D.Va. 1997).

239. *See generally id.*

240. *Id.* at 590.

241. *Id.*

242. *Id*. at 591 n.6.

243. The court in setting up the question to be addressed noted that although he was bound by United States v. Pelton, 835 F.2d 1067, 1074–75 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1988) (holding that the provisions of FISA are a reasonable accommodation between the governments need for intelligence information and the citizens right to privacy),"this Court addresses the narrow issue of physical searches under FISA as a matter of first impression." *Nicholson,* 955 F. Supp. at 590–91.

244. *Id.* at 591 n.6.

Amendment jurisprudence regards physical entry and electronic surveillance on an even plane, with each subject to the reasonableness requirement of the Fourth Amendment."[245] The court concluded that the physical searches in *Nicholson* were constitutionally indistinguishable from authorized electronic surveillance which had been unanimously upheld by all federal courts deciding the issue.[246]

The defendant also argued that the *ex parte* and *in camera* review authorized by FISA violated the due process clause of the Fifth Amendment[247] and the right to counsel clause of the Sixth Amendment of the Constitution.[248] The court, based on prior case law found that FISA did not violate the Fifth or Sixth Amendments by authorizing *ex parte* and *in camera* review.[249] The court was not persuaded by the defendant's Fifth Amendment equal protection clause argument that FISA is based on

---

245. *Id.*

246. *Id.*

247. U.S. CONST. amend. V. Amendment V of the United States Constitution provides:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Id.

248. *Nicholson,* 955 F. Supp. at 590. Amendment VI of the United States Constitution provides:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

U.S. CONST. amend.VI.

249. *Nicholson*, 955 F. Supp. at 592 (citing United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982) rejecting the argument that FISA violated the Fifth and Sixth Amendments).

invidious distinctions between agents of foreign powers as opposed to agents of domestic powers.[250]

In addition, the court held that FISA surveillance sanctioned by Article III judges did not violate the separation of powers doctrine.[251] The defendant argued that asking Article III judges to adjudicate search requests violated the separation of powers doctrine by allowing the judicial branch to interfere with executive branch authority.[252] The court followed an unbroken line of case law that consistently held that an Article III judge is properly acting in his judicial capacity when sitting on the FISA Court.[253] The defendant also argued that the surveillance and search violated the political question doctrine and had an impermissible chilling effect on First Amendment free speech.[254] The district court found these claims without merit citing *United States v. Duggan*[255] and *ACLU v. Barr*.[256] Regarding the defendant's First Amendment concern, the court noted that FISA explicitly provides that the exercise of free speech cannot be the sole basis for considering a United States person a foreign power or agent of a foreign power.[257] Thus, in the first case to test the constitutionality of the 1994 FISA amendments regarding physical searches, the district court applied pre-amendment FISA federal law to uphold the constitutional validity of the physical search provisions. There are several implica-

250. *Id*. at 592. The court held:

> [T]his Court holds that FISA does not violate any fundamental constitutionally-protected rights of surveillance subjects. Accordingly, this Court subjects FISA to rationality review and again adopts the reasoning of the Second Circuit in *Duggan*, holding that disparate treatment of foreign and domestic groups is rationally related to the "Act's purposes of attempting to protect the United States against various types of acts of foreign powers and to acquire information necessary to the national defense or the conduct of foreign affairs." Accordingly, FISA does not violate the Equal Protection Clause.

Id.

251. *Id*. at 592–93.

252. *Id*. at 592.

253. *Id*. at 593.

254. *Id.*

255. *See* United States v. Duggan, 743 F.2d 59, 74 (2d Cir. 1984).

256. *Nicholson,* 955 F. Supp. at 593. *See* American Civil Liberties Union v. Barr, 952 F.2d 457, 464 n.5 (9th Cir. 1991).

257. *Nicholson,* 955 F. Supp. at 593. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805 (1994).

tions to this holding. First, the court signaled that it would not draw a Fourth Amendment intrusiveness distinction between physical searc- hes and electronic surveillance. The court was not persuaded by the defendant's argument that physical searches of a residence are more intrusive than electronic surveillance. Second, this was the first court to hold that the FISA physical search provisions satisfy the requirements of the Fourth Amendment. Third, and most significantly, the court found physical searches and electronic searches to be "on an even plane" and to be subject to the same reasonableness requirement of the Fourth Amendment. Fourth, the court followed prior precedent involving electronic surveillance and applied that precedent to physical searches in holding the physical search provisions of FISA were a reasonable accommodation between the government's need for intelligence information and the citizen's right to privacy.

Therefore, in a very significant decision involving the applicability of the Fourth Amendment to physical searches under FISA, the court denied Nicholson's motion to suppress evidence.[258] While the legislative history of FISA demonstrates a clear congressional intent to restrain intelligence collection activities that were too intrusive, the court held that the physical search provisions under the Act were not intrusive and struck the appropriate balance between the government's interest in acquiring intelligence and protecting the rights of citizens.[259]

More recently, in *United States v. Usama Bin-Laden*,[260] the United States District Court for the Southern District of New York held that there is an exception to the warrant requirement for searches conducted abroad for foreign intelligence collection targeting foreign powers or their agents.[261] The district court also concluded that this exception applied to the physical search of an American citizen's home in a foreign country when there was probable cause to believe that the citizen was an agent of a foreign power and the purpose of the physical search was un-

258. *Nicholson*, 955 F. Supp. at 593.

259. *Id*. at 590 (quoting United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987)).

260. United States v. Usama Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000).

261. *Id*. at 277.

dertaken primarily for the purpose of foreign intelligence collection.[262]

The defendants in *Bin-Laden* were charged with offenses arising out of their participation in the international terrorist organization known as Al Qaeda.[263] These charges arose out of the defendant's involvement in the August 1998 bombings of the U.S. Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania.[264] El Hage, an American citizen and one of the defendants, sought the suppression of evidence seized from the physical search and electronic surveillance.[265]

The U.S. intelligence community identified several telephone numbers which were being used by people associated with Al Qaeda.[266] Several telephone numbers led directly to El-Hage.[267] Based on this information, the Attorney General authorized the collection of intelligence specifically targeting El-Hage.[268] In August of 1997, American and Kenyan officials conducted a search of the defendant's residence in Kenya and seized many items.[269] Defendant El-Hage and others sought suppression of the evidence which was seized during the warrantless search of his home in Kenya.[270] He also sought suppression of evidence derived from the electronic surveillance of several telephone lines, including his cellular phone.[271] In response to defendant's motion to suppress, the government argued that the searches were primarily for the purpose of foreign intelligence collection and not subject to the warrant requirement of the Fourth Amendment.[272]

Thus, the *Bin-Laden* case raised significant issues of first impression.[273] Among these was the applicability of the Fourth Amendment to searches conducted abroad for foreign intelligence purposes targeting United States persons believed to be agents

262. *Id*. at 285.
263. *Id*. at 268.
264. *Id.*
265. *Id.*
266. *Id*.
267. *Id*. at 269.
268. *Id*.
269. *Id*.
270. *Id*.
271. *Id*.
272. *Id*. at 270.
273. *Id*.

of a foreign power.[274] The court analyzed the cases finding an exception to the warrant requirement for foreign intelligence collection and concluded that the basis for the exception rested in the constitutional grant to the executive branch of power over foreign affairs.[275] The court also noted that "[w]arrantless foreign intelligence collection has been an established practice of the executive branch for decades."[276] Citing *United States v. Butenko*,[277] the court observed that in some circumstances the imposition of a warrant requirement may be a disabling burden on the executive branch.[278] Thus, in finding an exception to the warrant requirement to conduct physical searches of American citizens abroad who are targets of foreign intelligence collection, the court, quoting *United States v. Truong*[279] reasoned that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives [and] in some cases delay executive response to foreign intelligence threats."[280]

In recognizing the legitimacy of a warrant exception the court concluded that the power of the executive branch to conduct foreign intelligence collection would be significantly frustrated

---

274. *Id*.

275. *Id*. at 272.

276. *Id*. at 273. United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 310 (1972) (citing Brown & Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 103 (1985) (describing how warrantless electronic surveillance has been used by the Executive since the mid-1800s).

277. U.S. v. Butenko, 494 F.2d 593 (3d Cir. 1974).

278. *Bin Laden*, 126 F. Supp. 2d at 275 (citing *Butenko*, 494 F.2d at 605).

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

280. *Bin Laden*, 126 F. Supp. 2d at 275, (quoting *Truong*, 629 F.2d 908, 913 (4th Cir. 1980)). The Court in *Bin Laden* also noted the absence of a warrant procedure as a justification for the warrant exception under these circumstances.

> The final consideration which persuades the Court of the need for an exception to the warrant requirement for foreign intelligence collection conducted overseas is that there is presently no statutory basis for the issuance of a warrant to conduct searches abroad. . . In addition, existing warrant procedures and standards are simply not suitable for foreign intelligence searches.

Bin Laden at 275–76.

by the imposition of a warrant requirement.[281] Therefore, the court adopted the foreign intelligence exception to the warrant requirement for searches targeting foreign powers or their agents, which are conducted abroad.[282] The court went on to make it clear that this warrant exception applies to a foreign power or an agent of a foreign power and that the duration continues for as long as the primary purpose of the search is for foreign intelligence collection.[283] Thus, the defendant's motion to suppress evidence from the physical search of his Kenya residence and electronic surveillance was denied.[284]

While the United States Supreme Court has not addressed the issue of warrantless physical searches in the context of FISA, every federal court that has considered the issue has concluded, consistent with the jurisprudence before the 1994 FISA amendments, that the Fourth Amendment warrant requirements are flexible depending on the interests of the government at stake.[285] Where the governmental interests involve national security and the targets of the physical searches and electronic surveillance are for the purposes of foreign intelligence collection, then an exception to the usual warrant requirement is justified based on the expansive power of the executive branch in foreign affairs.

Through FISA, the Congress and the courts have struck the appropriate balance between individual privacy and governmental interests. They have narrowly set out the circumstances under which a surveillance order can be issued and limited the dissemination of collected information that falls outside of the general purpose of the authorized surveillance. For example, warrantless searches are only authorized in the narrowest of circumstances and for a limited time period against specific targets.[286] To the extent that a United States person is in-

281. *Bin Laden*, 126 F. Supp. 2d at 277.
282. *Id.*
283. *Id*. at 278.
284. *Id*. at 288. *Cf.* United States v. Squillacote, 221 F.3d 542, 555 (4th Cir. 2000) (holding that FISA surveillance was supported by probable cause and agents did not exceed scope of search warrant for defendant's residence).
285. *See generally* Brown & Cinquegrana, *supra* note 237, at 108–09, 114.
286. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1822 (1994).

volved without his or her consent, minimization procedures must be followed.[287]

C. The Anticipated Effects of the USA Patriot Act

1. The Effect of The USA Patriot Act on Civil Liberties

The national security interests of the U.S. government have dramatically changed because of the terrorist attacks of September 11, 2001.[288] In response to the terrorist attacks, Congress has passed several statutes that have been criticized as invading individual privacy for the sake of national security.[289] How far can the United States government go to protect national security? May it significantly intrude on individual privacy rights? The USA Patriot Act makes significant amendments to over fifteen statutes including FISA, Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[290] and the International Economic Emergency Powers Act.[291] The USA Patriot Act introduced "sweeping changes"[292] to the landscape of national security law by amending the following statutes:

- The wiretap statute (Title III of the Omnibus Crime Control and Safe Streets Act)[293]
- The Electronic Communications Privacy Act[294]
- The Computer Fraud and Abuse Act[295]

---

287. *Id*.

288. David E. Sanger & Steven Weisman, *Bush's Aides Envision New Influence in Region*, N.Y. TIMES, Apr. 10, 2003, at B11.

289. Seth Rosenfeld, *9-11-01; Looking Back, Looking Ahead; A Nation Remembers; Patriot Act's Scope, Secrecy Ensnares Innocent, Critics Say*, S.F. CHRON., Sept. 8, 2002, at A1.

290. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. § 2510 (West 2003).

291. International Economic Emergency Powers Act, 50 U.S.C. § 1701 (1977).

292. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15.

293. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. §§ 2510–2522. (West 2003).

294. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Electronic Communications Privacy Act, 18 U.S.C.A. § 2701 (West 2003).

- The Foreign Intelligence Surveillance Act[296]
- The Pen Register and Trap and Trace Statute[297]
- Money Laundering Control Act[298]
- Bank Secrecy Act[299]
- Right to Financial Privacy Act[300]
- Fair Credit Reporting Act[301]

The Congressional Research Service Report for Congress on the USA Patriot Act summarizes the statute generally, stating that it:

> Give[s] federal law enforcement and intelligence officers greater authority (at least temporarily) to gather and share evidence from wire and electronic surveillance; amend[s] federal money laundering laws, particularly those involving overseas financial activities; create[s] new federal crimes, increases the penalties for existing federal crimes, and adjusts existing federal criminal procedure, particularly with respect to acts of terrorism; modifi[es] immigration law [by] increasing the ability of federal authorities to prevent foreign terrorists from entering the U.S., to detain foreign terrorist suspects, to deport foreign terrorists, and to mitigate the adverse immigration consequences for the foreign victims of September 11; authorize[s] appropriations to enhance the capacity of immigra-

295. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030 (West 2003).

296. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (1994).

297. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Pen Register and Trap and Trace Statute, 18 U.S.C.A. § 3121 (West 2003).

298. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Money Laundering Control Act, 18 U.S.C.A. § 1956 (West 2003).

299. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Bank Secrecy Act, 31 U.S.C.A. §§ 5311–5330 (West 2003).

300. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Right to Financial Privacy Act 12 U.S.C.A. §§ 3401–3422 (West 2003).

301. Electronic Privacy Information Center, The USA Patriot Act *supra* note 15. *See* The Fair Credit Reporting Act, 15 U.S.C.A. § 1681 (a)-(v) (West 2003).

> tion, law enforcement, and intelligence agencies to more effectively respond to the threats of terrorism.[302]

The implementation of the USA Patriot Act has met a cool reception by many because of the potential for law enforcement abuse. This concern is captured succinctly by former Clinton White House Chief of Staff John Podesta's observations on the Act upon its adoption:

> The events of September 11 convinced…overwhelming majorities in Congress that law enforcement and national security officials need new legal tools to fight terrorism. But we should not forget what gave rise to the original opposition-many aspects of the bill increase the opportunity for law enforcement and the intelligence community to return to an era where they monitored and sometimes harassed individuals who were merely exercising their First Amendment rights. Nothing that occurred on September 11 mandates that we return to such an era.[303]

Mr. Podesta's concerns echo the proposition made at the beginning of this Article that the national security legal regime has come full circle. The same concerns that fueled the passage of FISA—overzealous law enforcement and intelligence collection abuse by the executive branch—are now the exact concerns levied at The USA Patriot Act's enforcement. These concerns may lead to significant changes to the USA Patriot Act currently being considered in the draft amendments titled USA Patriot Act II.[304] Mr. Podesta is not alone in his concern about the enforcement of the USA Patriot Act. Elliot Mincberg, Legal Director for People for the American Way has been very critical of Attorney General Ashcroft and the DOJ.[305] Mr. Mincberg asserts that "what the Justice Department has really done is to get things put into the law that have been on prosecutors' wish lists for years. They've used terrorism as a guise to expand law

---

302. CHARLES DOYLE, CRS REPORT FOR CONGRESS, TERRORISM: SECTION BY SECTION ANALYSIS OF THE USA PATRIOT ACT SUMMARY, (Dec. 10, 2001).

303. John Podesta, *The Good, the Bad, and the Sunset*, The Electronic Privacy Information Center, *at* www.epic.org/privacy/terrorism/usapatriot (last visited Oct. 8, 2003).

304. *See* Draft USA Patriot Act II, *supra* note 27.

305. Eric Lichtblau, *U.S. Uses Terror Law to Pursue Crimes from Drugs to Swindling*, N.Y. TIMES, Sept. 28, 2003, at A1 and A21 [hereinafter Lichtblau].

enforcement powers in areas that are totally unrelated to terrorism."[306]

Senator Russ Feingold, (D-Wisconsin) was the only Senator to vote against the Act.[307] He was particularly concerned about the Act's impact on civil liberties. He said:

> Now here's where my cautions in the aftermath of the terrorist attacks and my concerns over the reach of the anti-terrorism bill come together. To the extent that the expansive new immigration powers that the bill grants to the Attorney General are subject to abuse, who do we think is most likely to bear the brunt of the abuse? It won't be immigrants from Ireland, it won't be immigrants from El Salvador or Nicaragua it won't even be immigrants from Haiti or Africa. It will be immigrants from Arab, Muslim and South Asian countries. In the wake of these terrible events our [sic] government has been given vast new powers and they may fall most heavily on a minority of our population who already feel particularly acutely the pain of this disaster.[308]

The concerns about protection of civil liberties have become more pronounced recently in light of the DOJ's report to Congress in September 2003, citing more than a dozen cases not directly related to terrorism that used the USA Patriot Act's tools to gather evidence.[309] Many believe the USA Patriot Act gives the government too much authority to intrude on individual privacy.[310] Anthony Romero, Executive Director of the American Civil Liberties Union, said, "Once the American public understands that many of the powers granted to the federal government apply to much more than just terrorism, I think the opposition will gain momentum."[311] Senator Patrick J. Leahy of

306. *Id*.

307. Electronic Privacy Information Center, The USA Patriot Act, *supra* note 15.

308. Sen. Russell Feingold, *Statement on the Anti-Terrorism Bill*, (Oct. 25, 2002), Electronic Privacy Information Center, *at* http://www.epic.org/privacy/terrorism/usapatriot/feingold.html (last visited Oct. 8, 2003).

309. Report to Congress on Implementation of § 1001 of the USA Patriot Act (as required by § 1001(3) of Pub. L 107–56) (July 17, 2003), *available at* http://www.usdoj.gov/oig/special/03-07/index.htm; *see also* Lichtblau, *supra* note 305, at A1.

310. Lichtblau, *supra* note 306, at A1, A21.

311. *Id*. at A21.

Vermont, the ranking Democrat on the Judiciary Committee, said,

> the government is taking shortcuts around the criminal laws' …we did not intend for the government to shed the traditional tools of criminal investigation, such as grand jury subpoenas governed by well established precedent and wiretaps strictly monitored by federal judges.[312]

In contrast, the DOJ, maintains that it is using the expanded powers of the USA Patriot Act to fight terrorists.[313] Attorney General Ashcroft tried to defend the USA Patriot Act in September 2003 saying, "We have used these tools[314] to prevent terrorists from unleashing more death and destruction on our soil."[315] Thus, the tension between the USA Patriot Act and civil liberties has reached a boiling point and may ultimately only be resolved by the judiciary.

2. The Effect of the USA Patriot Act on the Division Between the Intelligence and Law Enforcement Community

The USA Patriot Act also appears to erode the division between the intelligence and law enforcement communities.[316] The USA Patriot Act amended FISA to authorize consultation among federal law enforcement officers regarding information acquired from electronic surveillance or physical searches for terrorism and related investigations or protective measures.[317] The FBI is now allowed to request telephone and transactional

312. *Id*. (quoting Senator Leahy).

313. *Id.*

314. The Act provides enhanced surveillance procedures, such as, permitting the seizure of voice mail messages under a warrant; extending the scope of subpoenas for records of electronic communications to include the length of service utilized, temporary assigned network addresses, and the means and source of payment; providing district courts authority to allow a delay of required notice to the target of the warrant of the execution of a warrant if immediate notice may have an adverse result; and increasing the duration of FISA surveillance of a non-United States person who is an agent of a foreign power. *See* USA Patriot Act, Pub L. 107–56 §§ 209, 210, 213, 115 Stat. 272, 283 (to be codified at 50 U.S.C. § 401(a)).

315. Lichtblau, *supra* note 305, at A1.

316. *See id*. USA Patriot Act, Pub L. 107–56, § 504, 115 Stat. 272, 283 (to be codified at 50 U.S.C. § 401(a)).

317. USA Patriot Act, Pub L. 107–56, § 504, 115 Stat. 272, 364–365 (to be codified at 50 U.S.C. § 401(a)).

records, financial records, and consumer reports in any investigation to protect against international terrorism or clandestine intelligence activities, as long as the investigation is not conducted solely on the basis of activities protected by the First Amendment.[318] Section 216 amends the federal criminal code to permit a court, upon application by a United States Attorney, to issue an *ex parte* order authorizing the installation and use of a pen register or trap and trace devices anywhere within the U.S.[319] The order would apply to any person or entity providing wire or electronic communication service in the U.S whose assistance may facilitate execution of an order.[320]

Section 403 of the USA Patriot Act also raises individual privacy concerns.[321] It amends the Immigration and Nationality Act[322] to require the Attorney General and the FBI to provide the Department of State and the Immigration and Naturalization Service ("INS") with access to specified criminal history extracts to determine if an applicant for a visa has a criminal history.[323] Section 403 also directs the Attorney General and the Secretary of State to develop technology standards to identify visa applicants.[324] This new technology will be the basis for an electronic system of law enforcement and intelligence sharing available to consular, law enforcement, intelligence and federal border inspection personnel.[325] The USA Patriot Act further amends the Immigration and Nationality Act to broaden the scope of aliens ineligible for admission and to allow for the deportation of aliens due to terrorist activities.[326] Section 414 requires that the Attorney General and Secretary of State implement an integrated entry and exit data system for airports, seaports, and land border ports of entry, with all deliberate speed.[327] These amendments are additional examples of the dis-

318. *Id.* § 505, 365–66.
319. *Id.* § 216, 288–90.
320. *Id*.
321. *Id.* § 403, 343–45.
322. Immigration and Nationality Act, 8 U.S.C. §1105 (1952).
323. USA Patriot Act, Public Law No. 107–56, § 403, 115 Stat. 272, 343–45.
324. *Id.* § 403, 343–45.
325. *Id*. § 403, 344.
326. *Id.* § 411, 345–50.
327. *Id.* § 414, 353–54.

integration of the wall between intelligence collection and law enforcement.

The metaphorical "wall" referred to is the wall between the intelligence community and law enforcement that evolved through judicial interpretations of FISA.[328] The wall concept is based on judicial assumptions linked to the statutory minimization procedures of FISA.[329] These minimization procedures were designed to restrict the use of foreign intelligence material collected during electronic surveillance.[330] The DOJ explains the development of the wall best in its report to Congress:

> The wall between intelligence and law enforcement resulted from perceived differences between legal authorities that permit the Federal Bureau of Investigation (FBI) to engage in electronic surveillance in the course of its foreign counterintelligence function, on the one hand, and its law enforcement function on the other. These perceived differences created an artificial dichotomy between intelligence gathering and law enforcement, and FISA and Title III (which authorizes electronic surveillance in criminal cases).
>
> As enacted in 1978, FISA required that "the purpose of electronic surveillance is to obtain foreign intelligence information," a term that was (and still is) defined to include information necessary to the ability of the United States to "protect" against espionage or international terrorism. [citations omitted] Courts interpreted "the purpose" to mean "the primary purpose," and they interpreted "foreign intelligence informa-

328. *In re* Sealed Case No. 02–001, 310 F.3d 717, 720 (Foreign Intel. Surv. Rev. Ct. 2002).

329. *Id*. at 721.

330. *Id*. The FISA Review Court concluded that by minimizing retention,

> Congress intended that "information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed where feasible." [citation omitted]. Furthermore, "[e]ven with respect to information needed for an approved purpose, dissemination should be restricted to those officials with a need for such information." [citation omitted] The minimization procedures allow, however, the retention and dissemination of non foreign intelligence information which is evidence of ordinary crimes for preventative or prosecutorial purposes. [citation omitted] Therefore, if through interceptions or searches, evidence of "a serious crime totally unrelated to intelligence matters" is incidentally acquired, the evidence is "not…required to be destroyed."

Id. at 713.

> tion" to include information necessary to the ability of the United States to protect against espionage or international terrorism *using methods other than law enforcement*. Thus, according to this judicial interpretation of FISA, that statute could be used only if the primary purpose of surveillance or a search was the protection of national security using non-law enforcement methods; gathering evidence to support the prosecution of a foreign spy or terrorist could be a significant purpose of the surveillance or search, but only if that prosecutorial purpose was clearly secondary to the non-law enforcement purpose. As a practical matter, courts determined the government's purpose for using FISA by examining the degree of coordination between intelligence and law enforcement officials: the more information and advice exchanged between these officials, the more likely courts would be to find that the primary purpose of the surveillance or search was law enforcement, not intelligence gathering. This legal structure created what the [FISA Review Court] termed "perverse organizational incentives," expressly discouraging coordination in the fight against terrorism.[331]

In order to better obtain untainted FISA surveillance orders, the DOJ issued written guidelines in July 1995 that explained the necessity of maintaining limited contact between "[d]epa rtment personnel involved in foreign intelligence collection and those involved in law enforcement."[332] Thus, intelligence information could be "shared with prosecutors and criminal investigators only where that information established that a crime has been, is being, or will be committed."[333] When these requirements were met, "intelligence officials could seek approval to 'throw information over the wall.'"[334] The decisions regarding when to share information, however, rested entirely with intelligence officials, probably those least able to make an informed decision regarding what evidence is pertinent to a criminal case.[335]

---

331. United States Department of Justice Report to Congress on USA Patriot Act Implementation, *at* www.house.gov/judiciary/patriotlet051303.pdf at 13–14 (last visited Sept. 2003) (citation ommitted) [hereinafter DOJ Report].

332. *Id.* at 14.

333. *Id*.

334. *Id*.

335. *Id*. The DOJ described the wall arrangement in the following manner:

Thus, the wall was effective in preventing cooperation and coordination between intelligence and law enforcement, precisely the opposite of what is necessary in order to respond to quickly developing events involving terrorist activities within and outside of the U.S. Before the USA Patriot Act, the wall "often precluded effective and vital information sharing between the intelligence community and law enforcement."[336] The wall was the result of a judicial belief that it could approve applications for electronic surveillance as long as the government's objective was not "primarily" directed toward criminal prosecution of foreign agents.[337]

The Attorney General addressed this "wall" problem and others through provisions of the USA Patriot Act.[338] The Act made two significant changes to FISA. First, Section 218 removed the "primary purpose" language and replaced it with "a significant purpose" standard, permitting the use of FISA when "a significant purpose of the search or surveillance was foreign intelligence."[339] Second, the USA Patriot Act made it clear in Section 504(a) that "coordination between intelligence and criminal

---

> This policy proved to be wholly unworkable, as it entrusted the decision whether to share information with those who were not best positioned to apply the applicable standards. Only the law enforcement agents and prosecutors pursuing a particular criminal investigation can determine what evidence is pertinent to their case. In contrast, intelligence officials, who focus on the development of foreign intelligence for national security purposes rather than collecting and reviewing information for a particular criminal investigation, rarely consider the potential evidentiary value of a particular piece of information, unless such information self-evidently proves that a crime has been or may be committed. Thus, as a matter both of perceived legal imperative and of Department culture, it was impossible to permit full coordination between intelligence and law-enforcement personnel and to combine foreign intelligence and law enforcement information into a seamless body of knowledge. Indeed, law enforcement and intelligence personnel could not speak openly to each other and share information beyond the piecemeal sharing envisioned by the previously existing rules. As a result, sharing under these guidelines was relatively rare and generally not meaningful.

Id. at 14.

336. *Id*. at 13.

337. *Id*. at 13–14.

338. *Id*. at 14–15.

339. *Id.* at 15.

personnel was not the grounds for denying a FISA application."[340] Moreover, after the "enactment of the USA Patriot Act, the [Justice] Department promulgated new procedures…that expressly authorized — and indeed required — coordination between intelligence and law enforcement."[341] The legality of these new procedures became the subject of a FISA Court opinion which rejected them in part on May 17, 2002.[342] However, the new procedures were later approved by the FISA Review Court on November 18, 2002.[343]

The FISA Review Court held that the wall imposed by the various agencies as a result of judicial interpretation was not legally required, thus clearing the way for more information sharing between law enforcement and intelligence authorities.[344]

In the first constitutional test of the USA Patriot Act's amendment to FISA, the FISA Review Court considered the issue of whether the FISA Court decision imposing certain requirements and limitations on the grant of a FISA Court surveillance order, was consistent with the statutory requirements as amended by the USA Patriot Act.[345]

This case involved the request by the Attorney General for the FISA Court to "vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including the Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures."[346] The FISA Court, though it granted the requested surveillance order, imposed restrictions which the government contends are not required by FISA. The FISA Court required that the DOJ maintain the wall between law enforcement and intelligence collection, notwithstanding the USA Patriot Act amendments and the Attorney General's

340. *Id*.
341. *Id*.
342. *Id. See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002).
343. DOJ Report, *supra* note 331, at 15; *In re Sealed Case*, 310 F.3d 717.
344. *In re Sealed Case*, 310 F.3d at 720.
345. *Id*. at 719–20.
346. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 613.

new procedures expressly authorizing coordination between intelligence and law enforcement.[347]

Apparently, the FISA Court was concerned that the DOJ had misinterpreted the USA Patriot Act to provide more consultative authority than it thought FISA allowed. Accordingly, the court fashioned a "chaperone requirement,"[348] which provided that the Office of Intelligence Policy and Review ("OIPR") be invited to all consultative meetings between the FBI and the Criminal Division of the DOJ in order to coordinate efforts against international terrorism.[349]

The FISA Review Court did not agree with the FISA Court's interpretation of FISA. The FISA Review Court observed that the FISA Court's interpretation was based on an erroneous "assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement…"[350] However, the FISA Review Court held that the language of the statue did not support the assumption.[351] It agreed with the gov-

---

347. *Id.* at 625. The FISA Court modified the minimization procedures requested by the government as follows:

> Notwithstanding the foregoing, law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.

Id. at 625. The court further held:

> These modifications are intended to bring the minimization procedures into accord with the language used in the FISA, and reinstate the bright line used in the 1995 procedures, on which the Court has relied. The purpose of minimization procedures as defined in the Act, is not to amend the statute, but to protect the privacy of Americans in these highly intrusive surveillances and searches, "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

Id.

348. *In re Sealed Case*, 310 F.3d at 720.

349. *Id.* at 721.

350. *Id.*

351. *Id.*

ernment's argument that the judicially imposed wall was neither supported by the statute nor its legislative history.[352] Moreover, the court also agreed with the government's alternative argument that even if the "primary purpose test" was a legitimate construction of FISA prior to the passage of the USA Patriot Act, it was no longer a legitimate construction in light of the amendments to FISA.[353] Furthermore, the "significant purpose" language should now eliminate any doubt that the USA Patriot Act intended to allow information sharing whether or not the purpose was intelligence collection or criminal prosecution.[354]

The FISA Review Court noted that "it does not seem that FISA, at least as originally enacted, even contemplated that the FISA Court would inquire into the government's purpose in seeking foreign intelligence information."[355] The FISA Review Court noted that Congress required a certification of purpose under Section 1804 in order to prevent the practice of targeting a foreign power when the purpose of the surveillance was to collect information on an individual "for other than foreign intelligence purposes."[356] However, Congress placed no restriction on the government's use of collected foreign intelligence information to prosecute foreign intelligence crimes.[357] Both the House and Senate made it clear that prosecution was a way to address foreign intelligence crimes.[358]

Thus, the FISA Review Court concluded that the FISA Court incorrectly continued to rely on the wall concept based on a misinterpretation of the statute and the minimization procedures. Moreover, the FISA Review Court held that the FISA Court continued its erroneous interpretation despite the passage of the USA Patriot Act which amended FISA to change "'the pur-

352. *Id*. at 723.
353. *Id*. at 734.
354. *Id*. at 734–35.
355. *Id*. at 723. The FISA Review Court relied on sections 1804 and 1805 governing the standards a FISA court judge is to use in granting or denying a surveillance order. The Court concluded that nothing in the law required the court to inquire into the government's purpose in seeking foreign intelligence information. *Id.*
356. *Id*. at 725.
357. *Id*.
358. *Id*.

pose' language in 1804(a)(7)(B) to 'a significant purpose.'"[359] The USA Patriot Act amendments to FISA "expressly sanctioned consultation and coordination between intelligence and law enforcement officials."[360] Despite this express provision, the FISA Court relied upon the Attorney General's 1995 procedures as minimization procedures and continued to interpret FISA to require the wall.[361] Now armed with the new USA Patriot Act amendments, the Attorney General interpreted FISA much differently by approving "new Intelligence Sharing Procedures."[362] The Attorney General's new 2002 procedures "supersede[d] prior procedures and were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials."[363] These new procedures "eliminated the 'direction and control' test and allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding 'the initiation, operation, continuation, or expansion of FISA searches or surveillance.'"[364] Notwithstanding the Attorney General's position on the new procedures, the FISA Court ordered the adoption of the 2002 procedures "with modifications, as minimization procedures to apply in all cases."[365]

In light of the legislative history, the FISA Review Court concluded that there was no basis for the FISA Court to rely on the statute "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or

359. *Id*. at 728–29.
360. *Id*. at 729.
361. *Id*. at 730.
362. *Id.* at 729.
363. *Id*.
364. *Id*.
365. *Id*. The FISA Review Court held:

> Essentially, the FISA court took portions of the Attorney General's augmented 1995 procedures—adopted to deal with the primary purpose standard—and imposed them generically as minimization procedures. In doing so, the FISA court erred. It did not provide any constitutional basis for its action—we think there is none—and misconstrued the main statutory provision on which it relied. The court mistakenly categorized the augmented 1995 Procedures as FISA minimization procedures and then compelled the government to utilize a modified version of those procedures in a way that is clearly inconsistent with the statutory purpose.

Id. at 730. The FISA Review Court went on to discuss the statutory definition of the minimization procedures and their purpose. *See id*. at 731.

expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime."[366]

The conclusion reached by the FISA Review Court is supported by the government's actions seeking amendment to FISA through the USA Patriot Act. The government, in order to avoid the "primary purpose" requirement imposed by the courts sought an amendment to section 1804(a)(7)(B) which would only require "a purpose" rather than the "primary purpose" language.[367] Congress settled on the language "a significant purpose" so as not to give the government too much latitude.[368] Congress understood that, with this language, it was relaxing the "requirement that the government show that its primary purpose [in seeking the surveillance] was other than criminal prosecution."[369]

While no committee reports accompanied the USA Patriot Act, floor statements in the Senate demonstrate congressional intent.[370] Senator Patrick J. Leahy, Senate Judiciary Chairman said "[t]his bill… break[s] down traditional barriers between law enforcement and foreign intelligence. This is not done just to combat international terrorism, but for any criminal investigation that overlaps a broad definition of 'foreign intelligence.'"[371] The FISA Review Court also cited a statement made on the floor by Senator Feinstein, a supporter of the USA Patriot Act.[372]

---

366. *Id.* at 731.
367. *Id*. at 732.
368. *Id*.
369. *Id.*
370. *Id*.
371. *Id.*
372. Recognizing that the ultimate object of the USA Patriot Act was to make it easier to collect foreign intelligence information under FISA, Senator Feinstein said:

> Rather than forcing law enforcement to decide which purpose is primary — law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA. The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the

Congress was well aware that the USA Patriot Act would break down barriers between intelligence collection and law enforcement.[373] Senator Feingold expressed concern that the "significant purpose" amendment may be used to abuse Fourth Amendment protections.[374] However, the balance between national security and civil liberties was struck by Congress in the amendments to FISA. For those who were concerned that the amendments gave the government too much power, Senator Leahy suggested that "it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of foreign intelligence information."[375]

Thus, the FISA Review Court correctly concluded that the USA Patriot Act amendments to FISA,

> by using the word "significant," eliminated any justification for the FISA Court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test.[376]

The FISA Review Court further clarified its point by noting, "[o]f course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied."[377]

> potential target of a criminal prosecution. Many of the individuals involved in supporting the September 11 attacks may well fall into both of these categories.

Id. at 733 (citing 147 CONG. REC. S10591 (Oct. 11,2003)).

373. *See In re Sealed Case*, 310 F.3d at 733.

374. *Id*.

375. *Id*.

376. *Id*. at 735.

377. *Id*. The FISA Review Court added that "ordinary crimes may be inextricably intertwined with foreign intelligence crimes." For example, international terrorists may rob banks in order to finance the purchase of weapons of mass destruction. Evidence of the bank robbery should fall under the intelligence collection umbrella. However, the point is that the FISA process was not intended to be used solely as a "device to investigate wholly unrelated

3. The Effect on Individual Privacy Concerns

Armed with the USA Patriot Act, the DOJ, FBI and the intelligence agencies began combating global terrorism. The USA Patriot Act contains enhanced immigration provisions which, among other things, expands the "terrorism-related grounds" for deportation and permits the Attorney General to detain alien terrorist suspects for certain time periods.[378] As of January 11, 2002, the DOJ reported the detentions of 725 people.[379] The DOJ released the number of people being detained around the U.S, but did not release the names, arrest or custody information of the detained.[380] Only the nationality, date of arrest, legal charge, and date of charging document were released.[381] In response, advocacy groups including the American Civil Liberties Union ("ACLU") and the American-Arab Anti-Discrimination Committee have filed lawsuits against the government, demanding information about the detainees and requesting they be provided with lawyers.[382] These advocacy groups have alleged that in more than a dozen instances, thirty days had passed between the arrest of a detainee and the actual filing of a charge.[383] The ACLU and other advocacy groups are concerned that the detainees are being denied access to lawyers.[384] Detainees are only allowed visits if the person knows the name and alien number of the person.[385] However, the DOJ will not release this information.[386] Therefore, some immigration lawyers are concerned that many of those detained in the terrorism investigation that are not represented by counsel will

ordinary crimes." If the law is abused by those charged with its enforcement, they can and should be held accountable. *Id*. at 736.

378. H.R. Res. 3162, 107th Cong. (2001).

379. Tamar Lewin, *A Nation Challenged: The Detainees; Rights Groups Press for Names of Muslims Held in New Jersey*, N.Y. TIMES, Jan. 23, 2002, at A9.

380. *Id.*

381. *Id.*

382. *Id*.

383. *Id.*

384. *Id.*

385. *Id.*

386. *Id*.

agree to deportation as the quickest way to get out of jail.[387] One of the few ways immigration lawyers can help those detained is by giving "know your rights" presentations in jail.[388]

In its review of the USA Patriot Act, the ACLU criticized the Act as compromising Fourth Amendment protections. The ACLU argued that the Act eviscerated the probable cause requirement of the Fourth Amendment,[389] limited judicial oversight of telephone and internet surveillance,[390] put the CIA back in the business of spying on Americans,[391] and allowed for detention and deportation of people engaging in innocent associational activity.[392]

The ACLU argues that the USA Patriot Act limits judicial oversight of electronic surveillance by changing current law.[393] The ACLU contends that the low hurdle required to get telephone numbers traced during an ongoing criminal investigation is now imported, through the USA Patriot Act, to internet communications which involve more content than just telephone numbers alone.[394] Under current law, in order to obtain a pen register or trap and trace order, a law enforcement officer need only certify that the information sought is "relevant to an ongoing criminal investigation." [395] The order requires a "tele-

387. *Id.*

388. *Id.*

389. ACLU Freedom Network, *How the USA Patriot Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases* (Oct. 23, 2001), *at* http://archive.aclu.org/congress/1102301i.html [hereinafter Circumventing Privacy Protections].

390. ACLU Freedom Network, *How the USA Patriot Act Limits Judicial Oversight of Telephone and Internet Surveillance* (Oct. 23, 2001), *at* http://archive.aclu.org/congress/1102301g.html [hereinafter Judicial Oversight].

391. ACLU Freedom Network, *How the USA Patriot Act Puts the CIA Back in the Business of Spying on Americans* (Oct. 23, 2001), *at* http://archive.aclu.org/congress/1102301g.html [hereinafter Business of Spying on Americans].

392. ACLU Freedom Network, *How the USA Patriot Act Allows for Detention and Deportation of People Engaging in Innocent Associational Activity* (Oct. 23, 2001), *at* http://archive.aclu.org/congress/1102301h.html [hereinafter Detention and Deportation of People].

393. American Civil Liberties Union, *Surveillance Under the USA Patriot Act*, (Oct. 23, 2001), *at* http://www.aclu.org/Safeand Free/SafeandFree.cfm?ID=12263&c=206.

394. Nancy Chang, *The USA Patriot Act: What's So Patriotic About Trampling on The Bill of Rights*, Center for Constitutional Rights, *at* 5 http://www.ccr-ny.org/vz/Whatsnews/USA_Patriot_Act.pdf (last visited Oct. 7, 2003).

395. Judicial Oversight, *supra* note 390.

phone company to reveal the 'numbers dialed' to and from a particular telephone."[396] Under Section 216 of the USA Patriot Act, the judge has no discretion and "must grant the order upon receiving the certification."[397] "Section 216 of the USA Patriot Act…extend[s] this low threshold of proof to internet communications…"[398] These communications reveal more content than simply the numbers dialed to or from a telephone.[399] Unlike with telephone calls, the email address cannot always be easily separated from the content of the message.[400]

The ACLU also criticizes the USA Patriot Act for putting the CIA back in the business of spying on American citizens.[401] This concern is based on the fact that the FBI, CIA and NSA spied on student activists and others who opposed the war in Vietnam during the 1960s and 1970s.[402] FISA was passed in response to this abuse of power.[403] The USA Patriot Act "permits wide sharing of sensitive information gathered in criminal investigations by law enforcement agencies with intelligence agencies including the CIA, and the NSA, and other federal agencies including the INS, Secret Service and Department of Defense."[404] The ACLU fears that the USA Patriot Act gives the government a dangerously enhanced role in domestic intelligence gathering against U.S citizens,[405] a role that is "contrary to the statutory prohibition in the CIA charter barring it from engaging" in domestic security operations.[406]

Additionally, the ACLU contends that the Act allows for the deportation of people who engage in innocent First Amendment associational activity.[407] Current law under the Immigration and Nationality Act ("INA")[408] permits the Secretary of State to

396. *Id*.
397. *Id.*
398. *Id.*
399. *Id.*
400. *Id*.
401. Business of Spying on Americans, *supra* note 391.
402. *Id*.
403. *Id*.
404. *Id*.
405. *Id*.
406. *Id*. *See also* 50 U.S.C. § 403(3)(d)(1).
407. Detention and Deportation of People, *supra* note 392.
408. Immigration and Nationality Act, Pub. L. No. 88–414, 66 Stat. 163 (1952) (codified as amended at 8 U.S.C §§ 1101–1537 (2003)).

designate foreign groups with various procedural safeguards.[409] Section 411 of the USA Patriot Act "adds a new provision to INA Section 212(a)(3)(B) that permits designation of foreign and domestic groups without those procedural safeguards."[410] The ACLU contends that the USA Patriot Act creates a high risk of deporting innocent people for innocent associational activity with political groups that the government identifies as terrorist organizations.[411] Moreover, the ACLU argues that the Act puts the burden on the immigrant to prove that he did not know that his assistance would further terrorist activity.[412] The ACLU contends that this raises the specter of punishing innocent people for association with unpopular causes and is reminiscent of McCarthyism.[413]

While the ACLU's concerns are valid, they do not accurately reflect the intent of the legislative provisions or their operation. The USA Patriot Act enhances the ability of our intelligence and law enforcement communities to detect and prevent terrorist attacks.

Before the USA Patriot Act was adopted, local courts could only authorize wiretaps within the jurisdiction of the court.[414] Search warrants issued for email communications could not extend beyond the jurisdiction of the court issuing it.[415] For example, if a court in Tampa ordered a search warrant on Wile E.

---

409. Detention and Deportation of People, *supra* note 392.

410. *Id*. The ACLU states:

> Under this new power, the Secretary of State could designate any group that has ever engaged in violent activity a "terrorist organization"— whether it be Operation Rescue, Greenpeace, or People for the Ethical Treatment of Animals. The designation would render the group's non-citizen members inadmissible to the United States, and would make payment of membership dues a deportable offense. Under the [Act], people can be deported regardless of whether they knew of the designation and regardless of whether their assistance had anything to do with the group's alleged terrorist activity.

Id. *See also* Immigration and Nationality Act, 8 U.S.C.A. §§ 1101–1537. (West 2003).

411. Detention and Deportation of People, *supra* note 392.

412. *Id*.

413. *Id*.

414. Brigitte Anderson, *Backward March! The USA Patriot Act and the Bill or Rights*, *at* http://mtprof.msun.edu/Spr2002/BAWRart.html (last visited Oct. 4, 2003); *see also* H.R. Res. 3162, 107th Cong. §§ 206, 216–20 (2001).

415. *See id.*

Hacker, and during the course of the investigation a new email account is discovered on an internet service provider in San Francisco, law enforcement had no right to search that email account without obtaining an additional search warrant for that jurisdiction.[416] The USA Patriot Act changed these limitations by giving the courts permission to compel assistance from any communications provider in the U.S whose assistance is appropriate to further an investigation.[417] This allows federal investigators authority to execute the same search warrant on any downstream communication provider, regardless of the state in which it is operating.

Before the USA Patriot Act, the use of voice communications in email created a quandary for law enforcement because voice communications were protected by much more restrictive wiretap orders.[418] Law enforcement officers, even with a subpoena, could acquire a limited amount of information from an internet service provider.[419] Moreover, the Cable Act[420] set out an extremely restrictive set of rules governing law enforcement access to records held by local cable companies.[421] After adoption of the USA Patriot Act, law enforcement can obtain voice mail and other stored voice communications once a search warrant has been authorized.[422] The Act significantly expands the data that can be obtained from an internet service provider.[423] The Cable Act has also been amended to allow law enforcement to subpoena customer records without notification to the customer.[424]

Moreover, Sections 214 and 215 of the USA Patriot Act had the impact of liberalizing the use of pen register and trap and trace devices in addition to allowing law enforcement to require

416. *See id.*

417. Electronic Privacy Information Center, The USA Patriot Act, *supra* note 15.

418. *Id.*

419. *Id.*

420. The Cable Act, 47 U.S.C.A. § 521 (West 2003).

421. Electronic Privacy Information Center, The USA Patriot Act, *supra* note 15.

422. *Id*.

423. Judicial Oversight, *supra* note 390.

424. Electronic Information Privacy Center, USA Patriot Act, *supra* note 15.

the production of any tangible things relevant to an international terrorism investigation.[425]

Thus, the USA Patriot Act, through sweeping changes to existing law, removed many of the restraints on law enforcement that impeded investigation and apprehension of international terrorists. Significantly, the USA Patriot Act contains a sunset provision which operates to expire many of the "amendments enhancing surveillance authority on December 31, 2005."[426] Congress understood the concerns regarding enhanced government authority contained in the USA Patriot Act and provided for a reasonable amount of time within which to test the Act's application.[427] Congress is currently reviewing a draft USA Patriot Act II consistent with its commitment to monitor the implementation of the current Act.[428] Therefore, while the ACLU argues that any encroachment on the rights of citizens is cause for concern, the legislative efforts embodied in the USA Patriot Act are reasonable responses to the threat of terrorism.

IV. RECOMMENDATIONS

As a nation we are on the right track in combating terrorism. The legislative efforts of Congress are reasonable responses to an attack on the principles of freedom and self-determination. However, we will make mistakes as we address issues that we have not confronted before. A few observations illustrate this point. First, the nation is undergoing profound changes regarding personal and national security and in terms of its organizational and operational structure. The administration has undertaken a review of the FBI, CIA, NSA and established a Department of Homeland Security. Second, this country is on the cutting edge of the law. We are confronting novel legal issues that we have never directly addressed before in the context of a war against terrorism. Third, we are fighting a "war" that is unlike any war that we have ever fought before. We have no

425. *Id*. *See also* Circumventing Privacy Protections, *supra* note 389.
426. Electronic Information Privacy Center, USA Patriot Act, *supra* note 15.
427. *Id*.
428. Electronic Frontier Foundation, Patriot Act II (draft) (Jan. 9, 2003), *at* www.eff.org/censorship/terrorism_militias/patriot2draft.html (last visited Feb. 10, 2003).

enemy government and a global battlefield. In essence, the issues that we face are law shaping events.

We are shaping the law as the issues are presented, and under such circumstances there will be considerable disagreement over the appropriate course of action to take. The following recommendations nonetheless seem reasonable:

- Review the implementation of the USA Patriot Act and other laws to ensure that civil liberties are not undermined.
- Aggressively prosecute any violation of civil liberties or misuse of the laws passed to fight the war against terrorism.
- Place a sunset provision in all legislation passed in response to the war on terrorism and focus on those provisions that provide expanded powers to the U.S. Government.
- Ensure that the next wave of legislation goes through the full legislative process including full committee hearings and debate.
- Use the current Patriot Act to inform the development of USA Patriot Act II.
- Integrate the findings of the DOJ Report submitted to Congress in September 2003 regarding the implementation of USA Patriot Act I.
- Study the DOJ report, and make any abuses identified by it the focal point for amendments, revisions and new legislation.

V. CONCLUSION

The events of September 11th are hopefully the most horrific events many of us will ever have to live through. The administration declared that the terrorists responsible have committed an act of war.[429] The President advised the men and women in uniform to "get ready."[430] Indeed, the war against terrorism di-

429. R.W. Apple Jr., *After the Attacks: News Analysis; No Middle Ground,* N.Y. TIMES, Sept. 14, 2001, at A1.

430. James Risen, *After the Attacks: The Trail; Bush Tells the Military to "Get Ready"; Broader Spy Powers Gaining Support,* N.Y. TIMES, Sept. 16, 2001, at A1 [hereinafter Risen].

rected initially at Afghanistan, Al Qaeda and the Taliban government has been successful. The Taliban are no longer in power and some of Al Qaeda have been captured or killed. These terrorist attacks provide the best explanation for why the Fourth Amendment must be flexible when the government is engaged in foreign intelligence collection efforts. The United States Congress has passed a resolution authorizing the President to use

> all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.[431]

Additionally, as a result of the terrorist attacks, President Bush declared the U.S to be in a state of national emergency pursuant to the National Emergencies Act,[432] and by Executive Order authorized the Secretary of Defense to order up members of the Ready Reserve of the Armed Forces to respond to the continuing and immediate threat of further terrorist attacks.[433] President Bush indicated that the war against terrorism will not stop in Afghanistan, but will seek to destroy terrorists and those who support them wherever they may be.[434] Thus, the U.S. took the war on terrorism to Iraq, removed Saddam Hussein and his regime, and is now helping the Iraqi people to assume responsibility for their own future.[435]

More rigorous security measures are being implemented at the airports and Congress is now considering whether certain

---

431. Joint Resolution Authorizing the Use of Force Against Terrorism, S.J. Res. 23, 107th Cong. (2001).

432. National Emergencies Act, 50 U.S.C. § 1601 (1976).

433. *See* Exec. Order No. 13,223, 66 Fed. Reg. 48,201 (Sept. 14, 2001); Exec. Order No. 13,253, 67 Fed. Reg. 2791 (Jan. 16, 2002).

434. Joseph Curl, *Bush Advises Patience, Resolve in Extended War Against Terror*, WASH. TIMES, Sept. 30, 2001, at A3.

435. The United States Department of State, White House Progress Report on Global War Against Terrorism, *at* http://usinfo.state.gov/topical/pol/terror (last visited Sept. 28, 2003).

restrictions in place against assassinations should be lifted.[436] America has changed. R. James Woolsey, the former director of CIA said that "Washington has absolutely undergone a sea change in thinking . . . ."[437] Congressional leaders and those who oversee the national intelligence agencies are discussing ways to allow the intelligence agencies to combat terrorism more aggressively.[438] Congressional intelligence oversight committee leadership and former directors of the CIA now say Congress should consider easing some of the restrictions that have been placed on the intelligence agencies.[439] The terrorist attacks have provided a catalyst for change in the attitude of political leadership. The attitude now is reflected in comments like those of Senator Richard C. Shelby, Republican from Alabama and vice chairman of the Senate Intelligence Committee, who says, "we have got to be a hell of a lot more aggressive."[440] Former President George H. W. Bush, who served as director of the CIA under President Ford also commented about the "need to free up the intelligence system from some of its constraints."[441]

Thus, we have perhaps come full circle. This Article began with a review of the report of the Church Committee investigation and concerns of executive branch and intelligence agency abuse that led to the passage of FISA and implementation of Executive Order 12,333. These legislative and executive measures were meant to constrain the activities of the intelligence agencies and provide clear guidance on the constitutional limits of foreign and domestic surveillance. Today, because of the terrorist attacks the intelligence agencies will once again become a focal point as the U.S. searches for answers to the questions of why the intelligence community was not able to prevent attacks. It is possible, indeed likely that legislative solutions will be proposed to now untie the hands of the intelligence community in ways that may make it better able to combat terrorism.

---

436. Exec. Order No., 12,333, 3 C.F.R. 200, 213 (1982), *reprinted in* 50 U.S.C. § 401 (2000). Executive Order 12,333 § 2.11 provides that: "No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination." *Id.*

437. Risen, *supra* note 430, at A1.

438. *Id.*

439. *Id.*

440. *Id.*

441. *Id.*

These are precisely the questions that were debated as the USA Patriot Act was considered and ultimately passed into law. Some suggest that the USA Patriot Act is the most dangerous kind of law, a law that was passed in the heat of emotion and in reaction to a terrible tragedy. Once again, the question of striking the balance between national security and the Fourth Amendment will be center stage. However, now the context is not domestic surveillance of individuals, organizations and watch lists, but rather terrorism.

The appropriate balance between protecting the nation and civil liberties has been reached through the Congressional legislative efforts in its attempt to make it easier to combat terrorism. The genius of democratic society is that, though the system is not perfect, it does work. The constitutional checks and balances operate well to curtail overzealous executive, legislative or judicial activity regardless of the catalyst for overzealousness. As the Fourth Amendment cases have held, the purpose of the criminal law is to punish and deter crime. However, the purpose of intelligence collection is "stop or frustrate the immediate criminal activity."[442] The cases reviewed in this Article have found that the Congress struck an appropriate balance between national security and Fourth Amendment privacy concerns.

In the final analysis, it becomes very difficult to preserve civil liberties if the survival of the nation is in the balance. Without a secure nation, civil liberty becomes a function of those in control of the government. Thus, by preserving the nation we are better able to preserve freedom.

442. *In re Sealed Case* No. 02–001, 310 F.3d at 744 (Foreign Intel. Surv. Ct. 2002).