2008

The Protect America Act of 2007: A Framework for Improving Intelligence Collection in the War on Terror

Jeffrey F. Addicott
St. Mary's University School of Law, jaddicott@stmarytx.edu

Michael T. McCaul

THE PROTECT AMERICA ACT OF 2007: A FRAMEWORK FOR IMPROVING INTELLIGENCE COLLECTION IN THE WAR ON TERROR

JEFFREY F. ADDICOTT* & MICHAEL T. MCCAUL†

* Distinguished Professor of Law and Director, Center for Terrorism Law, St. Mary's University School of Law. B.A. (with honors), University of Maryland, 1976; J.D., University of Alabama School of Law, 1979; L.L.M., The Judge Advocate General's School of Law, 1987; L.L.M., University of Virginia School of Law, 1992; S.J.D., University of Virginia School of Law, 1994. Special recognition to Ahsan Nasar and Jennifer Sanchez, research fellows at the Center for Terrorism Law, for insight and expert research on this article.

† United States Representative, 10th Congressional District of Texas (2000–present), B.A. Trinity University, J.D., St. Mary's University, Senior Executive Fellows Program of the John F. Kennedy School of Government, Harvard University. Member of the House Committee on Homeland Security, Ranking Member of the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology and former Chairman of the Subcommittee on Investigations; Member of the House Foreign Affairs Committee; Member of the House Committee on Science and Technology; Member of the House Committee on Standards of Official Conduct; Assistant Republican Whip; Member of the House Republican Policy Committee; 109th Congress Freshman Liaison to the Republican Leadership; Vice Chairman of the U.S.-Mexico Inter-Parliamentary Group. Special recognition to Gene Irisari, Deputy Chief of Staff, Office of Congressman Michael McCaul, who supported this article with outstanding insight and expert research.

I. INTRODUCTION

> *In any civilized society the most important task is achieving a proper balance between freedom and order. In wartime, reason and history both suggest that this balance shifts to some degree in favor of order—in favor of the government's ability to deal with conditions that threaten the national well-being.*[1]
>
> William H. Rehnquist (1924–2005)

The Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act (Protect America Act)[2] was not the first revision of the Foreign Intelligence Surveillance Act (FISA),[3] nor will it be the last. When the United States Congress amended FISA by passing the Protect America Act in early August 2007, its action was unusually swift.[4] Although some critics chastised Congress for passing the bill,[5] there were

1. WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 222 (Alfred A. Knopf) (1998).

2. Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, Pub. L. No. 110–55, 121 Stat. 52 (2007) [hereinafter *Protect America Act*].

3. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (2000).

4. Open Congress, http://www.opencongress.org/bill/110-s1927/show (last visited Dec. 31, 2008). On August 1, 2007, Senator Mitch McConnell introduced the Protect America Act. *Id.* On August 3, 2007, the United States Senate passed Senator McConnell's bill by a comfortable 60–28 margin. *Id.* On August 4, 2007, the United States House of Representatives passed the bill by a similar margin of 227–183. *Id.* On August 5, 2007, President George W. Bush signed the Protect America Act into law. *Id.*

5. Some of the negative commentary on the Protect America Act contained the usual emotional *ad hominem* attacks against the government. *See, e.g.*, Aziz Huq, *Data Mining Our Liberties*, THE NATION, Aug. 7, 2007, http://www.thenation.com/doc/20070813/huq2 (arguing that "[c]ongressional oversight is even more laughable"). Huq writes, "Attorney General Gonzales, that paragon of probity and full disclosure, is required to report not on the program's overall operations, but solely on 'incidents of noncompliance.'" *Id.*

> George W. Bush has perfected the art of ramming ill-considered legislation through Congress by hyping emergencies that don't exist. He did it with the USA Patriot [sic] Act, the authorization for the Iraq war, the Military Commissions Act and now the 'Protect America Act' which amends the Foreign Intelligence Surveillance Act (FISA).

Marjorie Cohn, http://www.marjoriecohn.com (Aug. 9, 2007, 19:52 PST). Professor Cohn writes that in its response to "fear-mongering by the Bush administration, the Democrat-led Congress put its stamp of approval on the unconstitutional wiretapping of Americans." *Id.* To reflect their strong opposition to every provision of the bill, the American Civil Liberties Union (ACLU) issued a so-called "Fact Sheet" on the Protect America Act which they entitled the "Police America Act." ACLU Webpage, http://www.aclu.org/safefree/nsaspying/31203res20070807.html (last visited Dec. 31, 2008). Tim Lynch of the Cato Institute wrote: "[M]ost legislators put their reservations aside, curl up into the fetal position and say 'I am against terrorists too,' as they vote in

pragmatic reasons for favoring the Protect America Act. For example, it provided a positive framework for ensuring that the proper rule of law kept pace with the changes in technology, and it also rightly appreciated the emerging threats to national well-being from both al-Qa'eda-styled terrorism and other foreign machinations. If one couples the phenomenal technical advances in telecommunications technology with an acknowledgement of the growing threats to national security posed by hostile nations, it is obvious that the nation's intelligence community[6] must be properly equipped with the necessary tools to protect the nation. As Congress continues to revise and amend FISA, the Protect America Act of 2007 serves as a reminder of the many policy and legal tensions involved as the country grapples with balancing cherished civil liberties against the need for increased security and government accountability in this post-9/11 world.[7]

Accordingly, the purpose of this paper is to provide a brief overview of the efficacy of the Protect America Act in the context of the new ground it covers.[8] Given that the United States of America is in a state of war[9] with the al-Qa'eda terror

---

favor [of the Protect America Act]." Declan McCullagh and Anne Broache, *FAQ: How Far Does the New Wiretap Law Go?*, CNET NEWS.COM, Aug. 6, 2007, http://news.cnet.com/FAQ-How-far-does-the-new-wiretap-law-go—page-2/2100-1029_3-6201032-2.html?tag=mncol (last visited Dec. 31, 2008).

6. Several federal entities collect foreign intelligence, such as the National Security Agency, the Federal Bureau of Investigations, the Central Intelligence Agency, the Department of Defense, and the Department of Homeland Security among others. DIRECTOR OF NATIONAL INTELLIGENCE, DNI HANDBOOK, AN OVERVIEW OF THE UNITED STATES INTELLIGENCE COMMUNITY (2007), *available at* http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf.

7. The Center for Terrorism Law, St. Mary's University School of Law, San Antonio, Texas was established in 2003 in order to examine current and potential legal issues related to terrorism in light of the challenge of achieving and maintaining a proper balance between global security and civil justice. St. Mary's University School of Law, Center for Terrorism Law Webpage, http://www.stmarytx.edu/ctl/display.php?go=about (last visited Dec. 31, 2008). This goal is pursued through teaching; professional exchanges such as symposia and consultations; writing, commenting on and publishing written materials; training; and ensuring access to extensive information resources regarding terrorism. *Id.*

8. For an excellent overview of the debate see CRS Report RL34279, *The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues*, Elizabeth B. Bazan, (December 14, 2007, http://www.scribd.com/doc/3898188/RL34279).

9. The term "War on Terror" is one of many phrases used to describe the ongoing conflict between the United States of America and the al-Qa'eda terror network, al-Qa'eda-styled terror groups, and any state that sponsors or supports them. *See generally* President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001) [hereinafter *Bush*] (citing al-Qa'eda and the nations that support that "radical network of terrorists" as the enemy in the United States' War on Terror). The beginning of this War on Terror is set as September 11, 2001, when 19

network and al-Qa'eda-styled terrorists,[10] providing the U.S. intelligence community with the proper means to effectively combat the evolving threats to national security presents a legal and policy challenge that requires thoughtful attention from all three branches of the government.

II. OVERVIEW OF INTELLIGENCE COLLECTION

> *In a similar way, monitoring the electronic communications of foreign nationals outside this country who are believed to be affiliated with terrorist groups—particularly during a period of congressionally authorized war—is reasonable and thus not constrained by the Fourth Amendment.*[11] *And monitoring the electronic communications of foreign terrorists is even more reasonable when they are communicating with people inside the United States, who might be plotting the next catastrophic terrorist attack.*[12]
>
> Robert F. Turner

A. *Basic Framework of FISA*

As correctly stated in a 2007 CRS Report to Congress, FISA was "enacted in response [to] . . . revelations with regard to past abuses of electronic surveillance for national security purposes

---

members of the terrorist al-Qa'eda organization hijacked four domestic passenger jets while in flight and used them to kill approximately 3,000 people on U.S. soil. *Id.*

10. Prompted by the Supreme Court's 2006 holding in *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006), Congress passed the Military Commissions Act (MCA) in October 2006. Military Commissions Act of 2006, Pub. L. No. 109–366, 120 Stat. 2600, 10 U.S.C. § 948 (2006). Not only did the MCA provide affirmative legal approval to the creation of military commissions and affirm Congressional authorization for war, it also provided the clearest indication that Congress was utilizing the law of war to deal with certain "unlawful enemy combatants." *Id.* at § 948a.

The MCA defines these individuals as follows:

(i) a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qa'eda, or associated forces); or

(ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense.

Id.

11. H.S. v. Benkahla, 437 F. Supp. 2d 541, 544 (E.D. V. 2006).

12. *Hearing Before the H. Comm. on the Judiciary*, 109th Cong. (2007), p. 12, http://www.virginia.edu/cnsl/pdf/Turner-HJC-5Sept07-(final).pdf (last visited Dec. 31, 2008) (statement of Robert F. Turner).

and to the somewhat uncertain state of the law on the subject."[13] In tandem with Executive Order 12333[14] and Title III of the 1968 Omnibus Crime Control and Safe Streets Act,[15] FISA codifies in federal law the procedures associated with how the intelligence community conducts electronic surveillance and physical searches[16] for the acquisition of foreign intelligence for reasons of national security. Since its passage in 1978,[17] FISA has withstood a variety of legal challenges,[18] most of which concern possible Fourth Amendment violations.[19]

In passing FISA, Congress intended to strike an appropriate balance between the need to protect national security with the need to protect civil liberty rights of Americans. FISA was certainly never intended to adversely impact American government intelligence community activities directed at places or people outside of the United States.[20]

FISA created two layers of special courts: one to issue orders and the other to provide review. The Foreign Intelligence Surveillance Court (FISC) is a "secret" court comprised of

13. ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERVICE (CRS) REPORT FOR CONGRESS 5 P.L. 110–55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (AUGUST 23, 2007).

14. Exec. Order No. 12,333, 3 C.F.R. 213 (1982).

15. 18 U.S.C. §§ 2510–2520. Title III requires more due process than the constitutional minimum established by case law. Under Title III, a warrant must include: (1) identity of the applicant; (2) specific details of the criminal offense; (3) particular descriptions of the facilities to be employed, including the types of electronic communications to be intercepted and the identity of the person whose conversation is to be intercepted; (4) description of less intrusive law enforcement techniques that had failed or would fail if employed; (5) specific time period of the electronic surveillance: and (6) all previous applications for a warrant for the same surveillance. *Id.* § 2518.

16. *See* 50 U.S.C. §§ 1821–1829 (2000) (amending FISA in 1994 to provide authorization to conduct physical searches in addition to electronic surveillance).

17. *See, e.g.*, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans, Book II*, S. Rep. No. 94-755, at 169 (1976) (discussing the political background and context of the FISA statute), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIa.htm.

18. *See* Richard Henry Seamon & Willam Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 359–65 (2005) (tracing Fourth Amendment challenges to warrantless surveillance before and after the passage of FISA).

19. U.S. CONST. amend. IV.

> 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.

20. *See infra* notes 36–68 and accompanying text.

eleven non-disclosed federal district court judges appointed by the Chief Justice of the Supreme Court.[21] Since these appointed judges are federal district court judges, the FISC is a proper Article III court.[22] A FISC judge rules on the submitted intelligence community applications[23] for court orders authorizing or denying electronic surveillance and physical searches.[24] The Foreign Intelligence Surveillance Court of Review (FISCR) is also a secret court and consists of three non-disclosed federal district or federal appellate judges with the power to review FISC actions.[25]

The basic mechanics for how the FISC court order process works reveal a stringent system of agency checks and cross-checks prior to submission to the FISC judge. An application to conduct an electronic surveillance is initiated by a federal intelligence community officer. After going through a variety of internal agency bureaucratic procedures and rules, culminating with the approval of the Attorney General, the application is then presented under oath to a FISC judge.[26] The central language in the application must clearly address a number of issues to include the following: (1) how the target of the electronic surveillance is to be identified[27] as well as the information relied on by the government to demonstrate that the target is either a "foreign power"[28] or an "agent of a foreign power;"[29] (2) the type of surveillance which will be used;[30] (3) the minimization procedures to be employed;[31] and (4) certification by a high-ranking Executive Branch official that he specially determines that the information sought is "foreign intelligence

21. 50 U.S.C. §§ 1803(a)–1803(b) (2000).

22. U.S. CONST. art. III, § 1.

23. *But see* 50 U.S.C. § 1824(e)(1)(A) (2000) (providing authority to the U.S. Attorney General to conduct an "emergency" surveillance or search provided that FISC approves said activity within 72 hours).

24. *Id.*

25. 50 U.S.C. §§ 1822(b)–1822(d) (2000).

26. 50 U.S.C. § 1805(a)(2) (2000).

27. 50 U.S.C. § 1804(a)(2).

28. 50 U.S.C. §§ 1804(a)(3)(A). The statutory term "foreign power" includes a group engaged in international terrorism "whether or not [that group is] recognized by the United States." 50 U.S.C. §§ 1801 (a)(1), 1801(a)(4) (2000).

29. 50 U.S.C. § 1804(a)(3)(A). The statutory term "agent of a foreign power" includes one who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power." 50 U.S.C. § 1801(b)(2)(C) (2000).

30. 50 U.S.C. § 1804(a)(7).

31. 50 U.S.C. § 1804(a)(4). The term "minimization" is defined at 50 U.S.C. §§ 1801(h)(1)–1801(h)(2).

information"[32] and that "a significant purpose" of the electronic surveillance or search is to obtain foreign intelligence information.[33] In order to issue a court order authorizing the surveillance, the FISC judge reviewing the application must specifically determine that there is probable cause to believe that the target of the surveillance or search is a foreign power or an agent of a foreign power and that a significant purpose of the electronic surveillance or search is to collect foreign intelligence. Nevertheless, the representations in the application must be accepted unless the FISC judge finds that they are "clearly erroneous."[34] In the case of a person residing in the United States the FISC judge must also determine that the target of the surveillance is not being considered an agent of a foreign power based on activities protected by the First Amendment.[35]

B. *Constitutional Limitations of FISA*

While the FISA rules regarding collection of foreign intelligence in the United States are clearly spelled out in statute, the question of whether or not the Executive Branch's Article II[36] power trumps FISA restrictions has never been decided by the United States Supreme Court.[37] In other words,

32. 50 U.S.C. §§ 1804 (a)(6)(A)–1804(a)(6))(B) (2000), 1823(a)7(A), 1823(a)(7)(B) (2000).

33. *Id.* Following the terror attacks of September 11, 2001, Congress passed an exhaustive piece of anti-terror legislation entitled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2000). Among the many much needed changes to existing laws and regulations, the USA PATRIOT act amended FISA to change the requirement then found in 50 U.S.C. § 1804 (a)(7)(B) from "the purpose" of the surveillance or search to "a significant purpose." 50 U.S.C. § 1804(a)(6)(B) (2000).

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

35. U.S. CONST. amend. I. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." *Id.*

36. U.S. CONST. art. II, § 2, cl. 1. The primary language setting out executive authority is derived from Article II of the Constitution which provides that the President "shall be the Commander in Chief of the Army and Navy of the United States."

37. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936). Although Article II of the Constitution specifically names the President as the Commander-in-Chief, it does not mention the term "foreign affairs" as an executive power. Nevertheless, the fact that the President has the primary responsibility for engaging in foreign affairs is widely accepted. *Curtiss-Wright Export Corp,* the most frequently cited Supreme Court case that speaks to the matter, states:

> Not only, as we have shown, is the federal power over external affairs in origin and essential character different from that over internal affairs, but participation in the exercise of the power is significantly limited. In this vast external realm, with its important, complicated, delicate and manifold

despite the fact that a string of presidents have operated under the parameters of FISA when conducting foreign intelligence, it is still an open question from the perspective of the Supreme Court as to whether the President's Article II power exempts him from the Fourth Amendment warrant requirements when foreign intelligence is conducted, even if that foreign intelligence collection takes place in the United States proper. Thus, despite the limitations that FISA places on the President's ability to conduct warrantless wiretaps on foreign agents in the United States, no act of Congress can "outlaw" a constitutional power of the Executive Branch that exists independently of the powers of the other two branches of government.[38]

The first Supreme Court rulings associated with warrantless electronic surveillance came about in two 1967 cases, *Katz v. United States*[39] and *Berger v. New York*.[40] Both cases addressed the matter in the context of domestic criminal activity. In *Katz*, the Court held that any warrantless electronic surveillance, including wiretaps, that violates a reasonable expectation of privacy, is per se unreasonable under the Fourth Amendment."[41] Quickly following suit, the court in *Berger* set out a series of requirements for the issuance of a valid warrant by a judge or magistrate: (1) the warrant must describe with particularity the communications to be heard; (2) there must be a showing of probable cause that a crime has been committed, or is being committed; (3) there must be a time limit on the surveillance; (4) the suspect(s) whose communications are intercepted must be named; (5) a return report must be made to the court regarding the communications intercepted; and (6) electronic surveillance must cease when warrant-approved information is

---

> problems, the President alone has the power to speak or listen as a representative of the nation. He makes treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude, and Congress itself is powerless to invade it.

Id.

38. "By the Constitution of the United States, the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character, and to his own conscience." Marbury v. Madison, 5 U.S. 157, 165-66 (1803); *see also* INS v. Chadha, 462 U.S. 919 (1983) (declaring legislative vetoes unconstitutional).

39. Katz v. U.S., 389 U.S. 347 (1967).

40. Berger v. New York, 388 U.S. 41 (1967).

41. *Katz*, 389 U.S. at 357 (ruling that warrantless searches "conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions").

obtained.[42]

While *Katz* and *Berger* were landmark cases in the area of domestic criminal electronic surveillance activities, it is important to understand that the *Katz* majority refused to address the need for a warrant in cases associated with national security, stating at footnote 23 of the opinion that "safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[43] *Berger* made no reference to issues of national security vis-à-vis electronic surveillance.

The last time that the Supreme Court spoke at any length on the issue of the President's authority to conduct warrantless electronic surveillance in foreign intelligence instances was in 1972. In *United States v. United States District Court* the Court was asked to rule on a number of legal challenges brought on behalf of three defendants who had been convicted of conspiracy to bomb a Central Intelligence Agency (CIA) office in Michigan.[44] The plot had been discovered by use of an electronic wiretap authorized by then Attorney General John Mitchell without a judicial warrant. While the Court ruled that warrantless domestic electronic surveillance related to ordinary domestic law enforcement was unconstitutional,[45] it clearly drew a strong distinction between such common criminal investigations and the matter of legitimate foreign intelligence electronic surveillance.[46] When discussing a compelling interest of the government in national security matters, the Court indicated that there could be circumstances in which a specific electronic surveillance could be conducted without a judicial warrant if it was "reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[47] The strong distinction between conducting electronic surveillance on domestic targets with no ties to a "foreign power" and the President's surveillance power towards actions of "foreign powers, within or without this

42. *Berger*, 388 U.S. at 55–57.

43. *Katz*, 389 U.S. at 358 n.23.

44. United States v. U.S. Dist. Court for E. Dist. of Mich., S, Div., 407 U.S. 297 (1972) [hereinafter *Keith*].

45. *Id.* at 320.

46. *Id.* at 308.

47. *Id.* at 322–23.

country"[48] was set out at both the beginning of the per curium opinion and at the end. At the beginning, the Court stated: "Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."[49] Near the end of the opinion, the Court wrote:

> We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We 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.[50]

If the *Keith* decision passed on the opportunity to fully address the President's independent constitutional authority to conduct warrantless electronic surveillance when the target was a foreign power or an agent of a foreign power, subsequent federal circuit courts have been rather consistent in their view. Every U.S. Court of Appeals to address the matter—both prior to and after *Keith*—has held that the Executive Branch, by virtue of the President's inherent authority under Article II, has the power to conduct warrantless electronic surveillance for national security reasons related to foreign powers and their agents.[51]

In the 1965 case of *United States v. Brown*, the Fifth Circuit Court of Appeals affirmed the use of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes.[52] One of the issues before the court involved the legality of incidental statements from an American citizen that were intercepted as a result of the warrantless government wiretap.[53] The court upheld the warrantless wiretap, which obtained the incidental statements, due to the "President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national

48. *Id.* at 308.

49. *Id.*

50. *Id.* at 321–22.

51. *See also* United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970) (stating that the law in question did not limit the President of the United States from taking any necessary steps to protect national security), and *FISA for the 21st Century: Hearing on S. 2453 Before the S. Comm. on the Judiciary*, 109th Cong. (2006) (statement of Bryan Cunningham, Principal, Morgan & Cunningham, LLC), ("Federal appeals courts ruling on the President's authority to conduct foreign intelligence electronic surveillance operations have recognized the President's constitutional preeminence in the collection of foreign intelligence to protect our national security.").

52. United States v. Brown, 484 U.S. 418 (5th Cir. 1973).

53. *Id.* at 424–425.

security in the context of foreign affairs."[54]

In 1974, the Third Circuit followed suit when it decided in *United States v. Butenko* that warrantless electronic surveillance was lawful so long as the primary purpose of the activity was to obtain foreign intelligence.[55] The court in *Butenko* acknowledged that the complex nature of society today makes sophisticated techniques necessary "for gathering intelligence information where national security is involved."[56]

The Ninth Circuit Court of Appeals next considered the issue of warrantless electronic surveillance in the case of *United States v. Buck*.[57] In affirming the legality of such electronic surveillance when authorized by the Executive to conduct surveillance of foreign powers and agents of foreign powers, the court specifically recognized this authority as an "exception to the general warrant requirement."[58]

The only post-FISA circuit court case dealing with the President's power to conduct warrantless electronic surveillance is the 1980 Fourth Circuit case of *United States v. Truong Binh Hung*.[59] At issue was the legality of a warrantless wiretap authorized by the Attorney General to target a Vietnamese national living in the United States. In the course of the year-long electronic surveillance process, information was obtained that ultimately assisted in the prosecution of Truong Dinh Hung for passing classified U.S. government documents to an informant for delivery to officials of the Socialist Republic of Vietnam.[60] Following *Keith*, the district court judge divided the electronic surveillance activity into two parts—admitting into evidence those that were done to collect foreign intelligence information and excluding those later surveillance activities that were done for domestic law enforcement. In reviewing, the circuit court affirmed the President's constitutional power to utilize warrantless wiretaps as a "'foreign intelligence' exception to the Fourth Amendment's warrant requirement."[61] Understanding that countering "foreign threats to the national

54. *Id.* at 426.
55. United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974).
56. *Id.* at 624.
57. United States v. Buck, 548 F.2d 871 (9th Cir. 1977).
58. *Id.* at 875.
59. United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).
60. *Id.*
61. *Id.* at 912.

security require the utmost stealth, speed, and secrecy,"[62] the Fourth Circuit affirmed that no warrant was required because of the Executive's "constitutional prerogatives in the area of foreign affairs,"[63] so long as the purpose of the warrantless electronic surveillance was directed at "a foreign power, its agents or collaborators."[64]

The only other federal case of significant impact[65] is *In re Sealed Case,* issued by the FISA Ct. Rev. in 2002.[66] In concluding that the USA PATRIOT Act[67] allowed domestic use of intercepted evidence obtained by electronic surveillance so long as a significant international foreign intelligence objective was in view at the interception, the FISA Court of Review unanimously stated:

> The *Troung* court, as did all other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.[68]

III. THE PROVISIONS OF THE PROTECT AMERICA ACT

> *As the head of the nation's Intelligence Community, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist or other threats to our security.*[69]
>
> J. Michael McConnell

The purpose of the Protect America Act was to provide an immediate update to FISA in order to give the intelligence community the necessary tools required to gather information

62. *Id.* at 913.

63. *Id.* at 912.

64. *Id.* at 915.

65. *But see* Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975), cert. denied, 425 U.S. 944 (1976) (noting, in a plurality opinion requiring a warrant to wiretap a domestic target that was not an agent of a foreign power, that "an analysis of the polices implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional.").

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

67. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2000).

68. *In re Sealed Case,* 310 F.3d at 742.

69. *Foreign Intelligence Surveillance Act and Implementation of the Protect America Act: Hearing Before the S. Comm. on the Judiciary,* 110th Cong. 3 (2007) (statement of J. Michael McConnell, Director of National Intelligence).

about potential foreign enemies.[70] The preamble to the bill states this goal as follows: "To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information."[71]

The legislative history reveals that the bill was introduced in the Senate on August 1, 2007,[72] passed in the Senate on August 3, 2007,[73] passed in the House on August 4, 2007,[74] and signed into law by President Bush on August 5, 2007.[75] The vote in the House of Representatives was 227 to 183,[76] with 41 Democrats supporting and 181 opposing; 186 Republicans voted in support and 2 opposed. The vote in the Senate was 60 in favor and 28 opposed with 15 Democrats supporting and 28 opposing; 45 Republicans voted to support and none voted to oppose.[77]

As the Director of Intelligence Mike McConnell related in his September 25, 2007 statement before the Senate Judiciary Committee, the heart of the Protect America Act is the provision that does away with the need to obtain "court approval when the target of the acquisition is a foreign intelligence target located *outside* the United States."[78] To accomplish this, the Protect America Act limits the construction of the term "electronic surveillance"[79] so that it does not apply to a person reasonably

70. Fact Sheet: The Protect America Act of 2007, http://www.whitehouse.gov (last visited August 29, 2007).

71. Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, Pub. L. No. 110-55, § 1927, 121 Stat. 552 (2007).

72. GovTrack.us Web Page, http://www.govtrack.us/congress/bill.xpd?bill=s110-1927 (last visited Dec. 31, 2008).

73. *Id.*

74. *Id.*

75. ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERVICE (CRS) REPORT FOR CONGRESS, SUMMARY (AUGUST 23, 2007).

76. GovTrack.us Web Page, http://www.govtrack.us/congress/bill.xpd?bill=s110-1927 (last visited Dec. 31, 2008).

77. *Id.*

78. *Foreign Intelligence Surveillance Act and Implementation of the Protect America Act: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 9 (2007) (statement of J. Michael McConnell, Director of National Intelligence).

79. 50 U.S.C. § 1801(f)(2008):

> Prior to the enactment of the Protect America Act of 2007, "electronic surveillance" had been defined for purposes of FISA to mean:
>
> (f) "Electronic surveillance" means—
>
> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person6 who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has

believed to be located outside the United States. Section 105A of FISA states: "Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States."[80] The Protect America Act thus restores FISA to its original intent and is closer in line with judicial case law regarding the Executive's power to conduct intelligence operations directed at foreign targets.[81] The Protect America Act allows collection of communications completely foreign in nature without obtaining a warrant[82]

Nevertheless, the mechanics of the process still include notifying the FISA Court of any warrantless surveillance operation within seventy-two hours of authorization.[83]

---

a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

80. Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, Pub. L. No. 110-55, Sec. 105A, 121 Stat. 552 (2007).

81. *See* United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974) (holding that that warrantless electronic surveillance was lawful so long as the primary purpose of the activity was to obtain foreign intelligence).

82. *See Foreign Intelligence Surveillance Act and Implementation of the Protect America Act: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 3, 9 (2007) (statement of J. Michael McConnell, Director of National Intelligence) (explaining that the definition of electronic surveillance does not include a person thought be outside the United States which means no court approval is needed to target an individual outside the United States).

83. Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, Pub. L. No. 110-55, §105B(a), 121 Stat. 552 (2007). Section 105B begins by providing that:

> [*n*]*otwithstanding any other law*, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information *concerning* persons reasonably believed to

The Protect America Act also requires communications providers to cooperate with the Attorney General and the Director of National Intelligence to provide whatever technical support might be necessary to acquire information associated with the targeting of individuals outside the United States.[84] In tandem with this requirement, the Protect America Act provides protection for third-parties from private lawsuits arising from any government assistance that the third-parties may provide.[85]

In regards to reporting requirements, the Protect America Act at section 4 requires the Attorney General to report to Congress any incidents of noncompliance as well as the number of directives issued. Moreover, semi-annually officials are to update these committees as to the number of directives that were issued in that year under the authority conferred by section 105B.[86]

---

be located outside of the United States if the DNI and Attorney General determine that based upon the information provided to them, that—

(1) there are *reasonable procedures* in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and *such procedures* will be subject to review of the Court pursuant to section 105C of this Act;

(2) the acquisition does not constitute electronic surveillance;

(3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

(4) *a significant purpose* of the acquisition is to obtain foreign intelligence information; and

(5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

84. *Foreign Intelligence Surveillance Act and Implementation of the Protect America Act: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 3, 10 (2007) (statement of J. Michael McConnell, Director of National Intelligence). The Attorney General and Director of National Security may direct a person to provide the Government with all information, facilities, and assistance necessary and in a manner that will protect secrecy. Further it is provided that the Government shall compensate said person for providing said information, facilities, and assistance. If the person fails to comply as directed, the Attorney General may invoke the aid of the Foreign Intelligence Surveillance Act (FISC) to compel compliance with the directive. A FISC order can be issued requiring the person to comply under threat of contempt of court if the directive is lawful. However, the person in receipt of a directive may challenge its legality by filing a petition with the petition pool of the FISC.

85. *Id.*

86. Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, Pub. L. No. 110-55, §4, 121 Stat. 52, 50 U.S.C. §1805C (2000). The statute states:

Finally, the Protect America Act requires FISA Court involvement in determining that reasonable procedures are used in ascertaining whether a target is outside the United States.[87] New section 105C deals specifically with the required submissions and the assessments that are to be made by the FISC regarding the acquisitions conducted pursuant to new section 105B.[88] Clearly, the necessity of this function stems from the new statutory definition of "electronic surveillance." Accordingly, the Attorney General is required to submit to the FISA Court[89] the procedures that the government employs in determining that the acquisitions authorized under 105B do not constitute electronic surveillance. Moreover, within 180 days after enactment of the Protect America Act, the FISA Court must assess whether the government's determination under section 105B(1) is founded upon procedures that are "reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance" are clearly erroneous.[90] The FISA Court is required to enter an order approving the continued use of the procedures, unless they are to be found to be clearly erroneous. However, should the FISA Court find the government's determination to be clearly erroneous, new procedures must be submitted "within 30 days" or any acquisitions under section 105B must cease.[91] Any order issued by the FISA Court finding said procedures to be clearly erroneous may be appealed to the FISCCR.[92] If the FISCCR finds that the order by the FISA Court was properly entered, the government may then seek Supreme Court review through the filing of a petition for writ of certiorari.[93] During the

---

> On a semi-annual basis the Attorney General shall inform the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning acquisitions under this section during the previous 6-month period.

87. *Foreign Intelligence Surveillance Act and Implementation of the Protect America Act: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 3, 10 (2007) (statement of J. Michael McConnell, Director of National Intelligence).

88. Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, Pub. L. No. 110-55, §4, 121 Stat. 52, 50 U.S.C. §1805C(a) (2000).

89. *Id.* § 1805C(c).

90. *Id.* § 1805C(b).

91. *Id.*

92. *Id.*

93. *Id.* § 1805C(d) (saying that if the Court of Review affirms the FISC order, the Court of Review must immediately prepare a written statement of each of the reasons for

review process, the acquisitions affected by the FISA Court order at issue may continue.

IV. CRITICISMS OF THE PROTECT AMERICA ACT

> *The so-called "Protect America Act of 2007," which we are calling the "Police America Act," allows for massive, untargeted collection of international communications without court order or meaningful oversight by either Congress or the courts.*[94]

Just as calls for increased security must be weighed against protecting cherished civil liberties, all criticisms of increased security measures such as the Protect America Act must be weighed against a realistic understanding of the threat to national security. Although the United States has not suffered another mega-terror strike on the homeland since the al-Qa'eda attack of September 11, 2001, the threat to the United States posed by al-Qa'eda and al-Qa'eda-like Islamic terrorists has not diminished.

A. *Understanding the Threat*

Cloaking itself in a "religious"[95] fanaticism, these al-Qa'eda-styled jihadists are set on using violence against the United States in order to kill tens of thousands, if possible.[96] This point cannot be seriously debated or doubted. The 2004 bipartisan 9/11 Commission Report found that the United States is facing a loose confederation of people who believe in a perverted stream of Islam and are busy building the groundwork for decades of struggle.[97] Similarly, the July 2007 National

---

its decision. Should the government file a certiorari petition, that written record would be transmitted under seal to the U.S. Supreme Court).

94. American Civil Liberties Union, ACLU Fact Sheet on the "Police America Act," http://www.aclu.org/safefree/nsaspying/31203res20070807.html (last visited Dec. 31, 2008).

95. *See, e.g.*, Jeffrey F. Addicott, *The Misuse of Religion in the Global War on Terrorism*, 7 BARRY L. REV. 109 (2006) (discussing how al-Qa'eda-styled terrorism conducts murder in the name of religion and the concept of jihad as an obligation to engage in "holy war").

96. *Id.*

97. 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 51 (2004).

> [Bin Ladin and al-Qa'eda] say that America had attacked Islam; America is responsible for all conflicts involving Muslims. Thus Americans are blamed when Israelis fight with Palestinians, when Russians fight with Chechens, when Indians fight with Kashmiri Muslims, and when the Philippine government fights ethnic Muslims in its southern islands. America is also held responsible for the governments of Muslim countries, derided by al Qa'eda as "your agents." Bin Ladin has stated flatly, "Our fight against these governments is

Intelligence Estimate (NIE) entitled: Terrorist Threat to the U.S. Homeland, spells out the clear and present danger posed by al-Qa'eda against the United States.[98]

---

not separate from our fight against you." These charges found a ready audience among millions of Arabs and Muslims angry at the United States because of issues ranging from Iraq to Palestine to America's support for their countries' repressive rulers.

Id.

98. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, NATIONAL INTELLIGENCE ESTIMATE, THE TERRORIST THREAT TO THE U.S. HOMELAND 6 (2007); *see also* FOREIGN INTELLIGENCE SURVEILLANCE ACT AND IMPLEMENTATION OF THE PROTECT AMERICA ACT: HEARING BEFORE THE S. COMM. ON THE JUDICIARY, 110th Cong. 7–9 (2007) (statement of J. Michael McConnell, Director of National Intelligence). In his September 25, 2007 testimony before the Senate Judiciary Committee, the Director of National Intelligence, J. Michael McConnell, highlighted the following threats:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'eda, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.
- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'eda to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.
- l-Qa'eda is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess that the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'eda senior leadership since 9/11, we judge that al-Qa'eda will intensify its efforts to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.
- We assess that al-Qa'eda will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'eda will probably seek to leverage the contacts and capabilities of al-Qa'eda in Iraq.
- We assess that al-Qa'eda's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.
- We assess that al-Qa'eda will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.
- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.
- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

As a consequence of the War on Terror,[99] both the Executive and Legislative Branches of government have employed a wide variety of new legal and policy initiatives to address the threat posed by both al-Qa'eda-styled terrorism and rogue states who possess weapons of mass destruction.[100] Designed to disrupt terrorist networks and prevent future terrorist attacks from occurring, these new tools include such things as: the passage of the USA PATRIOT Act;[101] the creation of the Department of Homeland Security;[102] the establishment of United States Northern Command, in Colorado;[103] the passage of the Military Commissions Act of 2006,[104] the use of military force against the Taliban government in Afghanistan,[105] the preemptive use of military force against the Iraqi regime of Saddam Hussein,[106] and the resulting indefinite detention of suspected terrorists who are illegal aliens and unlawful enemy combatants. In short, the central challenge that the United States faces, along with the rest of the civilized world, is how to realistically engage these

---

Id.

99. *Bush, supra* note 9.

100. *See* NATIONAL STRATEGY TO COMBAT WEAPONS OF MASS DESTRUCTION (2002), *available at* http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf (describing the United States' strategy utilizing counterproliferation, nonproliferation, and consequence management to address the threat of use of Weapons of Mass Destruction against the United States and its friends and allies).

101. *See* USA PATRIOT Act, 115 Stat 272. The bill passed in the Senate by a vote of 98-1. 147 CONG. REC. S11059–60 (2001). The House of Representatives passed their version by a vote of 357-66. House Vote on H.R. 3162 (Oct. 24, 2001), http://clerk.house.gov/evs/2001/roll398.xml.

102. Homeland Security Act of 2002, 6 U.S.C. §§ 101–C12 (2006).

103. "U.S. Northern Command (USNORTHCOM) was established Oct. 1, 2002 to provide command and control of Department of Defense (DoD) homeland defense efforts and to coordinate defense support of civil authorities." About U.S. Northern Command, http://www.northcom.mil/About/index.html (last visited Nov. 7, 2008).

104. 10 U.S.C. § 948 (2006).

105. Authorization for Use of Military Force Joint Resolution, S.J. Res. 23, 107th Cong. (2001). This resolution was passed by every member of the Senate and every member of the House of Representatives, save one. *Id.* Among other things, the Congressional Resolution recognized the authority of the President " . . . under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* The resolution also stated:

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

Id.

106. The Iraq War was authorized by a Congressional use of force resolution which specifically found that Iraq supported international terrorism and was in development of weapons of mass destruction. Authorization for the Use of Military Force Against Iraq Resolution of 2002, H.R.J. Res. 114, 107th Cong. (2002).

new enemies while providing the highest level of protection for American civil liberties.

One issue is certain in this debate: due to the universalist designs of al-Qa'eda and al-Qa'eda-styled militant Islam, the use of a one-dimensional criminal justice system designed to respond to terrorist attacks can neither confront nor contain an ideology of hate able to infect thousands of followers and deploy secretive terrorist cells across the globe. Nevertheless, the use of the government's new methodologies designed to thwart terrorist attacks and similar aggression has caused some to challenge such measures as illegal (note that there is a vast difference between calling something wrongheaded and calling it illegal). It is no surprise then that a deep fissure runs through the legal and political debate.

As in all wars, the need for accurate intelligence is crucial to success. In the War on Terror, where the enemy fights asymmetrically, i.e., the terrorist does not wear a uniform, does not carry his arms openly, nor does he abide by any of the humanitarian precepts of the law of war,[107] the need for accurate intelligence is absolutely paramount. For instance, security measures to stop the terrorist at the airport are far too late. The terrorist must be stopped prior to ever approaching the airport. Since the terrorist "hides amongst us" and generally denies any affiliation with terrorism (if one can engage in the murder of civilians, one can certainly be expected to lie and deceive), any antiterrorism[108] efforts must be built around the gathering of

107. The basic goal of the law of war is to limit the impact of the inevitable evils of war by: "(1) protecting both combatants and noncombatants from unnecessary suffering; (2) safeguarding certain fundamental human rights of persons who fall into the hands of the enemy, particularly prisoners of war, the wounded and sick, and civilians; and (3) facilitating the restoration of peace." DEPARTMENT OF ARMY, FIELD MANUAL 27-10: THE LAW OF LAND WARFARE, para. 2 (1956), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/law_warfare-1956.pdf (last visited Dec. 31, 2008). The current corpus of the law of war consists of all those treaties and customary principles that are applicable to war. *Id.* The 1949 Geneva Conventions serve as the primary source for the law of war and cover four basic categories: (1) Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; (2) Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, August 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; (3) Geneva Convention Relative to the Treatment of Prisoners of War, August 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; and (4) Geneva Convention Relative to the Protections of Civilian Persons in Time of War, August 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 287.

108. Antiterrorism involves all those steps and actions taken to decrease the probability of a terrorist attack. It is proactive and can involve electronic surveillance, modeling techniques and the use of other intelligence gathering devices. By contrast,

solid intelligence, to include electronic surveillance. In this light, one of the more controversial actions taken by the Bush Administration was the Terrorist Surveillance Program (TSP), a secret program authorized after the September 11, 2001 terror attacks and revealed to the public in December of 2005. The TSP employed the use of warrantless wiretaps to monitor the messages of foreigners that passed through communication links in the United States as well as those communications where one party was operating outside the United States.[109] While the exact details of the TSP remain classified, several media reports purportedly contained details of the program, which suggested the use of data mining and traffic analysis.[110] Additionally, public statements made by administration officials indicate that the TSP involved interceptions when there was "a reasonable basis to conclude that one party to the communication is a member of al-Qa'eda, affiliated with al-Qa'eda, or a member of an organization affiliated with al-Qa'eda, or working in support of al-Qa'eda."[111] When the TSP was revealed to the general public by the New York Times newspaper,[112] the Bush Administration made a policy decision to put the program under the purview of the FISA court.[113] Then, in 2007, when one of the FISA judges issued a secret ruling questioning some aspects of the revised process,[114] the Bush Administration pushed for swift Congressional legislation to address the

---

counterterrorism involves those tactical measures taken in response to an actual terrorist attack.

109. Press Release, The White House, Setting the Record Straight: Democrats Continue to Attack Terrorist Surveillance Program (Jan. 22, 2006) (on file with St. Mary's University School of Law, Center for Terrorism Law).

110. *See* Shane Harris, *How Does the NSA Spy?*, NAT'L J., Jan. 20, 2006, at 47, 49 (noting that although the precise details of the NSA remain classified, press reports indicate that data mining and traffic analysis technologies are being employed).

111. Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (December 19, 2005).

112. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. (The article cites anonymous government officials regarding the use of warrantless eavesdropping on persons inside the United States "based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qa'eda and other terrorist groups.").

113. "I was pleased that the [Bush] Administration submitted the [Terrorist Surveillance Program] TSP to the FISA Court, and that the Court had found a way to issue an order approving this surveillance." 153 CONG. REC. S4480-01 (daily ed. Apr. 16, 2007) (statement by Sen. Feinstein).

114. House Minority Leader John A. Boehner stated, "There's been a ruling, over the last four or five months, that prohibits the ability of our intelligence services and our counterintelligence people from listening in to two terrorists in other parts of the world where the communication could come through the United States." Greg Miller, *Court Puts Limits on Surveillance Abroad*, L.A. TIMES, August 2, 2007, at A16.

concerns.[115] Apparently, the concerns led the FISA court to conclude that communications between two individuals located outside the United States could no longer be intercepted without a FISA warrant if those communications passed through an internet switch (node) located in the United States.[116] After an intense push by the Bush Administration to secure at least temporary amendments to the statutory framework of FISA, before Congress adjourned from their summer legislative sessions, the end result was the passage of the Protect America Act.[117]

B. *Challenging the Protect America Act*

A review of most of the reasoned critics of the Protect America Act shows that concerns fall into two general categories. On the one hand, some critics argue that the statute is not only too confusing but that the very terminology and language utilized in the statute opens the door to possible abuse by the intelligence community.[118] In part, criticism is fueled by the fact that FISA itself is too complicated, but the argument is actually more properly seen as a fear of unintended consequences. On the other hand, some believe that the Executive Branch's provision of warrantless wiretap authority is simply unconstitutional, ab initio, particularly when it involves any person, place, or thing associated with the United States proper.

To take the complex and make it understandable is always a daunting task. Again, critics who fall into the first category generally lament the complexity of FISA and then wonder about the impact of the language revisions set forth in the Protect America Act. For instance, in Suzanne Spaulding's September 25, 2007 testimony before the Senate Judiciary Committee hearing on "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?," she argued in particular that the Protect America Act was flawed because it altered the definition of the term "electronic surveillance" to exclude persons reasonably believed to be

115. For an overview of the chronology see CRS Report RL34279, *supra* note 8, at 7–8.

116. Miller, *supra* note 114, at A16.

117. *See* David Ignatius, *Dangerous Logjam on Surveillance*, WASH. POST, Sept. 30, 2007, at B7 (providing an overview of the chronology of events).

118. *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (2007) (statement of Suzanne E. Spaulding, Principal, Bingham Consulting Group).

outside the United States. Spaulding testified: "First, I would urge Congress to avoid trying to accomplish objectives by changing definitions. The terms in FISA not only appear throughout this complex statute [FISA]; they are also referenced in or inform other laws, Executive Orders, directives, policies, etc. The risk of unintended consequences is significant."[119]

Other objections for those who fall into the first category range from the fact that the Protect America Act does not contain the word 'terrorism' or 'terrorist'[120] to the use of the language "notwithstanding any other law" contained in section 105B of the Act,[121] which some interpret as free license to authorize such actions as "intercepting US mail between two people inside the United States, so long as the government reasonably believes the letter discusses, at least in part, someone outside the US."[122]

Of course, to anyone even marginally familiar with the FISA rules, the criticism that the Protect America Act is somehow disingenuous because it fails to mention the term "terrorism" and instead only mentions "foreign" powers is a shallow argument. The term "foreign power" as defined by 50 U.S.C. § 1801 (a) (4)-(5) includes "a group engaged in international terrorism or activities in preparation therefore" or "a foreign-based political organization, not substantially composed of United States persons."[123] Thus, foreign powers include terrorists,[124] and al-Qa'eda and any similar terrorist organization is properly classified as a "foreign power."[125]

Similarly, the fears that the government will engage in

---

119. *Id.*

120. Strengthening FISA, *supra* note 118.

> Despite this new law having been explained to the American public as necessary to protect them from the next terrorist attack, none of the intelligence collection it authorizes has to be related in any way to terrorism. It applies to any "foreign intelligence," a term which has been amended over the years to include a very broad range of information.

Id.

121. *Id.*; Protect America Act of 2007, *supra* note 2, § 105B.

122. *Id.*

123. 50 U.S.C. § 1801(a)(4)–(5).

124. *See* United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000) (holding that a FISA application to perform electronic surveillance of a foreign power or its agents must specify reasons for this conclusion).

125. *See* United States v. Bin Laden, 126 F. Supp. 2d 264, 278 (S.D.N.Y. 2000) (holding that an international terrorist organization was properly classified as a foreign power for purposes of foreign intelligence gathering).

"reverse targeting," i.e., conduct electronic surveillance without a warrant on a person "reasonably believed to be located outside of the United States," but in reality focusing on a person located in the United States,[126] are vastly overstated. Such activity is not authorized by the Protect America Act and would be a clear violation of 50 U.S.C. § 1801(f)(1).[127]

Those in the second category generally craft their arguments in terms of analyzing the gathering of any and all electronic surveillance purely from a domestic law enforcement viewpoint, rejecting the notion that the Executive Branch has independent authority to conduct electronic surveillance of foreign powers for purposes of national security.[128] In turn, most would also reject the notion that the United States is at "war," treating the matter as distracting rhetoric. For them, the phrase "War on Terror" is more similar to the Reagan era "war on drugs" or the Johnson era "wars on poverty." It is not a "real" war and therefore the use of, for example, military commissions, warrantless wiretaps of foreign powers, and other wartime powers of the government would be quite illegal and unconstitutional.

In his September 25, 2007, testimony before the Senate Judiciary Committee, James Dempsey exemplified the second category of critics. Dempsey engaged in a lengthy critique of the Protect America Act, admitting that while the Supreme Court has never ruled on the issue of whether warrantless electronic surveillance to collect foreign intelligence in the context of national security is constitutional, the federal circuit opinions set out in *Butenko*[129] and *Truong Dinh Hung*[130] indicate to him that the Protect America Act is an excessive exercise of authority. "The PAA falls short of the standards enunciated in Butenko and Truong. It is not limited to searches of the communications of foreign powers or agents of foreign powers. Searches under the PAA are not based on probable cause. They are not reasonably limited in duration."[131]

126. *Hearing on the Foreign Intelligence Surveillance Act Before the Permanent House Select Committee on Intelligence*, 110th Cong. (2007) (statement of Kenneth L. Wainstein, Asst. Attorney General, National Security Division, Department of Justice).

127. 50 U.S.C. § 1801(f)(1).

128. *See generally* Marjorie Cohn, http://majoriecohn.com (last visited Dec. 31, 2008).

129. United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974).

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

131. *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (2007) (statement of James Dempsey, Policy Director, Center for Democracy and Technology).

At the root of most reasoned critics of the Protect America Act is how new section 105A (of FISA) exempts from its statutory definition of electronic surveillance a broad class of surveillance activities. As a consequence, the scope of new activity outside of the old FISA framework is susceptible to varying constructions. This potential for confusion presents concern especially when viewed against the ambiguity within the text, which will necessarily require interpretation by the Executive Branch. In addition, because of the classified nature of the information involved, little opportunity exists for the public to discover the actual construction that the text received.

V. CONCLUSION

> *The most important weapon in the War on Terror is intelligence and our first line of defense is reliable intelligence.*
>
> Michael T. McCaul[132]

If the most important weapon in the War on Terror is intelligence, then America's first line of defense must be anchored on reliable intelligence. America's ability to gather and analyze intelligence is much greater than that of al-Qa'eda-

132. On July 9, 2008, the Senate passed by a 69–28 vote and President Bush signed into law H.R. 6304, "The FISA Amendments Act of 2008." The House of Representatives had previously adopted this legislation by a 293–129 vote on June 20, 2008. This bipartisan revision of FISA strengthens the government's ability to secure intelligence through monitoring phone conversations in a timely manner. A presidential administration must still obtain approval from a special FISA court in advance of conducting the surveillance. However, the law also gives the government flexibility during emergency situations to act first and seek retroactive approval from the court within seven days. Further, the law addresses the liability issues of telecommunication companies that provided information to our intelligence agencies after the tragedy of 9/11 by allowing the phone companies the ability to have such suits dismissed if they can prove they acted under orders from the president to detect or prevent a terrorist threat. The bill has built-in protections for Americans traveling abroad as well by prohibiting the intelligence community from intentionally targeting a U.S. citizen who is located outside of our borders under circumstances in which that person has a "reasonable expectation of privacy" and in which a warrant would be required in the U.S. The exceptions would be if there is FISA court approval or if the Attorney General has authorized an emergency acquisition.

Rep. McCaul said:

> This bill gives us the tools to capture foreign intelligence to protect America, and it closes the terrorist loophole in this country. Foreign terrorists abroad who are plotting to attack the United States will no longer be protected. The ability to listen in on potential foreign terrorists as they lay the groundwork for attacking the United States is essential to the security of this country and the safety of every American. . . . This takes the handcuffs off of our intelligence community and will undoubtedly save lives. This bill strikes the right balance between Americans' right to privacy and our country's needs to gather intelligence.

styled terrorists, and this advantage must be maintained. National security requires that every lawful means be employed to gather pertinent information. The American people rightfully expect that their government will continue to use every lawful tool available to protect them. In so doing, however, important safeguards are necessary to protect the civil liberties afforded under the Constitution's First and Fourth Amendments.

The Protect America Act, which was signed into law in August of 2007, closed the unacceptable intelligence gaps that had arisen because of the application of the FISA to foreign persons in foreign countries who were never intended to be covered by FISA. While operating under these unnecessary restrictions, intelligence agencies probably missed a significant portion of the information that was needed to protect the country and to pursue the al-Qa'eda-styled terrorists with whom America is at war.

While the debate on the efficacy of the Protect America Act will continue to color subsequent amendments to FISA, the Protect America Act allowed U.S. intelligence services the lawful right to resume collecting this information while still protecting the civil liberties of American citizens. The Protect America Act has contributed to efforts to detect and prevent another catastrophic terrorist attack on the United States. Terrorism-related arrests in England, Germany, and Denmark during the summer of 2007 lend proof to the need for timely intelligence collection.[133] In his 2007 testimony before the House Judiciary Committee, Director of National Intelligence, Admiral J. Michael McConnell testified that prior to the Protect America Act the Intelligence Community was not collecting 66% of the foreign intelligence information that it used to collect before legal interpretations required the government to obtain FISA court orders for overseas surveillance.[134] It is critical that the professionals at U.S. intelligence agencies have the ability and authority to collect information on foreign terrorists without

133. Terrorism and the Law, http://www.homeoffice.gov.uk/security/terrorism-and-the-law/; Danish Arrests 'Prevent Terrorism', http://edition.cnn.com/2007/WORLD/europe/09/04/danish.terror/index.html; Mark Lander, *German Police Arrest 3 in Terrorist Plot*, N.Y. TIMES, Sept. 6, 2007, *available at* http://www.nytimes.com/2007/09/06/world/europe/06germany.html.

134. Letter from Director of National Intelligence (DNI) J.M. McConnell to House Permanent Select Committee on Intelligence Chairman Silvestre Reyes (July 25, 2007) (*unclassified*).

cumbersome regulations requiring court orders and oversight that was never intended to be applied to such situations.

Since the passage of The Protect America Act, there have been numerous legislative attempts to scale back many of the important legislative provisions necessary to gather the best information possible to protect the nation from terrorism.[135] Some of these attempts would go far beyond the original intent of FISA. Contrary to some of the rhetoric, it is the members of al-Qa'eda, not American citizens that are the target of lawful intelligence gathering activities.

Legislative proposals should not stop intelligence professionals from conducting surveillance of foreign persons in foreign countries. Obviously, intelligence professionals cannot read the minds and intent of their targets so as to guarantee that those terrorist targets would not call the United States or a United States person. Furthermore, revisions in the FISA should not provide intelligence targets more protection than Americans receive under court-ordered warrants in organized crime and other criminal investigations.

The advances in telecommunications technology over the last 30 years mandate that FISA keep pace with the attendant heightened threat to national security. Terrorist tactics constantly change in response to American efforts to disrupt their plots, so essential intelligence tools and associated legal requirements for their use must be modernized. Although the Protect America Act served as a temporary fix, intelligence professionals need a long-term legal framework that provides certainty and clarity in order to aggressively collect the information necessary to protect the American people.

---

135. The 110th Congress has been very active in developing and considering measures to amend FISA since the Protect America Act, P.L. 110-55, was enacted into law on August 5, 2007. It expired on February 16, 2008, after passage of a 15-day extension to its original sunset date. P.L. 110-182, *available at* http://www.congress.gov/cgi-lis/bdquery/R?d110:FLD002:@1%28110+182%29. On November 15, 2007, the House of Representatives passed H.R. 3773, the RESTORE Act of 2007, *available at* http://www.congress.gov/cgi-lis/bdquery/z?d110:H.R.3773:. On February 12, 2008, the Senate passed S. 2248, *available at* http://www.congress.gov/cgi-lis/bdquery/z?d110:S.2248:, as amended, then struck all but the enacting clause of H.R. 3773, and inserted the text of S. 2248, as amended, in its stead. On March 14, 2008, the House passed an amendment to the Senate amendment to H.R. 3773. After months of intensive negotiations, on June 19, 2008, a compromise bill, H.R. 6304, The FISA Amendments Act of 2008, *available at* http://www.congress.gov/cgi-lis/bdquery/z?d110:H.R.6304:, was introduced in the House and was passed by the House the following day. The Senate passed the bill on July 9, and it was signed into law by President Bush on July 10, 2008 as P.L. 110-261.

Prior to the Protect America Act, Congress seemed content to ignore repeated warnings about the intelligence gap, even while cumbersome FISA restrictions hindered, for example, the search for three kidnapped American soldiers in Iraq, one of whom was killed while two are still missing in action.[136] Any legislative proposal that would bring back the nonsensical requirements for an advance court order to conduct overseas surveillance that unnecessarily delays intelligence collection must be rejected. Advance court review of intelligence activities against foreign targets does nothing to protect the civil liberties of Americans but does unduly hamper America's ability to fight terrorism.

Congress and the Executive must act to improve on the gains made by the Protect America Act and give permanent and effective legal authorities which will assist in closing existing intelligence gaps against potential foreign terrorists in foreign countries. In a floor speech given just prior to the adoption of the Protect American Act, Congressman Michael McCaul warned:

> Our most solemn duty in the United States Congress is to protect the American people; and while this bill [H.R. 3356, Improving Foreign Intelligence to Defend the Nation and the Constitution Act]—which weakens the Protect America Act—may be well intentioned, it fails to do that. In fact, just the opposite. It puts the American people in great danger. Before running for Congress, I worked in the Justice Department. I worked on national security, wiretaps and FISA. The intention of the FISA Act was never to apply to agents of a foreign power in a foreign country. It was to apply to agents of a foreign power in this country. This bill does just the opposite. It expands it to bar a collection of foreign intelligence on foreign targets in foreign countries. I am concerned that if we cannot collect intelligence overseas that we cannot protect our war fighter in the battlefield. We put them in danger, and we put the citizens of this country in danger. We all know that al Qaeda is looking at hitting us again. It may be very soon. And with the anniversary of 9/11 approaching, we must do everything we can to protect her.[137]

136. *See* Pauline Jelinek, *Senior Al-Qaida Leader Reported Killed In Airstrike*, ST. LOUIS POST-DISPATCH (MO), Sept. 29, 2007, at A30 (referring to the kidnapping).

137. Floor speech by Congressman Michael McCaul (TX-10) during floor debate of the H.R. 3356, Improving Foreign Intelligence to Defend the Nation and the Constitution Act (IMPROVE Act), August 3, 2007. This bill was considered by the House

the day before the debate on the Protect America Act. The IMPROVE Act failed on Suspension of the Rules by a vote of 218 to 207.