2-19-2007

The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment

Robert M. Bloom
Boston College Law School, robert.bloom@bc.edu

William J. Dunn
Boston College Law School, Class of 2006

Recommended Citation

Robert M. Bloom and William J. Dunn. "The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment." *William and Mary Bill of Rights Journal* 15, (2007): 147-202.

THE CONSTITUTIONAL INFIRMITY OF WARRANTLESS NSA SURVEILLANCE: THE ABUSE OF PRESIDENTIAL POWER AND THE INJURY TO THE FOURTH AMENDMENT

Robert Bloom* & William J. Dunn**

ABSTRACT

In the past year, there have been many revelations about the tactics used by the Bush administration to prosecute its war on terrorism. These stories involve the exploitation of technologies that allow the government, with the cooperation of phone companies and financial institutions, to access phone and financial records. This Article focuses on the revelation and widespread criticism of the Bush administration's operation of a warrantless electronic surveillance program to monitor international phone calls and e-mails that originate or terminate with a United States party. The powerful and secret National Security Agency heads the program and leverages its significant intelligence collection infrastructure to further this effort. Fueling the controversy are undeniable similarities between the current surveillance program and the improper use of electronic surveillance that was listed as an article of impeachment for former President Richard M. Nixon. President Bush argues that the surveillance program passes constitutional inquiry based upon his constitutionally delegated war and foreign policy powers, as well as the congressional joint resolution passed following the September 11, 2001 terrorist attacks. These arguments fail to supersede the explicit and exhaustive statutory framework provided by Congress and amended repeatedly since 2001 for judicial approval and authorization for electronic surveillance. The specific regulation by Congress based upon war powers shared concurrently with the President provides a constitutional requirement that cannot be bypassed or ignored by the President. The President's choice to do so violates the Constitution and risks the definite sacrifice of individual rights for speculative gain from warrantless action.

---

* Professor of Law, Boston College Law School. I wish to thank Hillary Massey, a student in the class of 2007 at Boston College Law School. I wish to gratefully acknowledge that the major portion of this article was done by my co-author, William J. Dunn. I also acknowledge with gratitude the generous support provided by the R. Robert Popeo Fund of Boston College Law School.

** J.D., Boston College Law School (2006). He spent three years as a civilian intelligence analyst for the Department of Defense prior to law school, which included a one-year assignment at the National Military Joint Intelligence Center in the Joint Chiefs of Staff, Pentagon, one year as a sensitive source reporting analyst and Central Intelligence Agency liaison for the Office of Naval Intelligence, and one year as an all-source Middle East analyst.

> When we're talking about chasing down terrorists, we're talking about getting a court order before we do so.
>
> —President George W. Bush[1]

> We join with you in the conviction that terrorism must be fought with the utmost vigor, but we also believe we must ensure this fight is conducted in a manner reflective of the highest American values.
>
> —Michael S. Greco[2]

INTRODUCTION

President George W. Bush responded to revelations that his administration conducted warrantless electronic surveillance of American citizens by stating, "As President and Commander in Chief, I have the constitutional responsibility and the constitutional authority to protect our country. . . . So, consistent with U.S. law and the Constitution, I authorized the interception of international communications of people with known links to Al Qaida . . . ."[3] President Bush attempted to defend this statement one month later by stating, "[O]ther Presidents have used the same authority I've had, to use technology to protect the American people."[4] This latter statement is certainly accurate, though its truth is both eerie and unsettling. Most notably, the argument that authorization for the warrantless surveillance is provided directly from the constitutional powers granted to the President harkens back to President Richard M. Nixon's statement that, "It's quite obvious that there are certain inherently government activities, which, if undertaken by the sovereign in protection of the interests of the nation's security are lawful, but which if undertaken by private persons, are not."[5]

---

[1] President's Remarks in a Discussion on the PATRIOT Act in Buffalo, N.Y., 40 WEEKLY COMP. PRES. DOC. 638, 641 (Apr. 26, 2004) [hereinafter Apr. 20, 2004 Remarks].

[2] Letter from Michael S. Greco, President, American Bar Association, to President George W. Bush (Feb. 13, 2006) (on file with American Bar Association), http://www.abanet.org/op/greco/memos/aba_donsurv_ltr_whthouse-0206.pdf.

[3] The President's News Conference (Dec. 19, 2005), 41 WEEKLY COMP. PRES. DOC. 1885, 1885 (Dec. 26, 2005) [hereinafter Dec. 19, 2005 Press Conference]. It should be noted that these revelations focused on international calls and e-mails in which one party to the communication was in the United States. Since this press conference, additional revelations with regard to the collection of phone call records have been reported. *See, e.g.*, Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at 1A.

[4] The President's News Conference (Jan. 26, 2006), 42 WEEKLY COMP. PRES. DOC. 125, 131 (Jan. 30, 2006) [hereinafter Jan. 26, 2006 Press Conference].

[5] David Frost, *Excerpts from Interview with Nixon About Domestic Effects of Indochina War*, N.Y. TIMES, May 20, 1977, at A16. Nixon justified the illegal nature of his authorized activities by appealing to presidential war powers. He stated, after referencing Abraham Lincoln's belief in the presidential power to take unconstitutional actions to preserve the nation, that

> it has been . . . argued that as far as a President is concerned, that in war

The comparison between the actions taken by President George W. Bush and Richard M. Nixon are not merely academic but are unnervingly similar in substance, scope, and perceived authority. Both included warrantless electronic surveillance of American citizens. Both were justified by the relative administrations through an appeal to national security imperatives. Both resulted in public outcry and congressional inquiry.[6]

President Nixon acted in the context of a nation transfixed with the war in Vietnam.[7] While the nation fixated on the deaths of over 50,000 Americans, President Nixon was preoccupied with the massive domestic protests that swept the country.[8] President Nixon believed that these protests were initiated by foreign elements.[9] To combat this national security threat, President Nixon launched a coordinated intelligence-gathering plan later named the Huston Plan.[10] The Huston Plan "advocated the systematic use of wiretappings, burglaries, or so-called black bag jobs, mail openings and infiltration against antiwar groups and others."[11] Though the Huston Plan itself lasted only five days before FBI Director J. Edgar Hoover terminated it, President Nixon's approval of the plan, despite his explicit awareness of its illegality, was listed in the Articles of Impeachment and cited by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee) in 1975 as "only an episode in the lawlessness which preceded and fol-

---

> time, a President does have certain extraordinary powers which would make acts that would otherwise be unlawful, lawful if undertaken for the purpose of preserving the nation and the Constitution, which is essential for the rights we're all talking about.

Id.

[6] *See id.*; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. The revelation of President Bush's warrantless electronic surveillance and blatant disregard of the requirements provided by the Foreign Intelligence Surveillance Act reportedly prompted United States District Judge James Robertson, a judge on the Foreign Intelligence Surveillance Court, to resign. Brian Knowlton, *Judge Quits Intelligence Court; Action Linked to Concern over U.S. Spying Without Warrants*, INT'L HERALD TRIB., Dec. 22, 2005, at 5.

[7] *See Huston Plan: Hearing on S. Res. 21 Before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 1 (1975) [hereinafter *Huston Plan Hearings*] (statement of Sen. Frank Church, Chairman, S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities). In addition, the assassination of President John F. Kennedy led the Secret Service to task the National Security Agency (NSA) with the collection of information under the national security justification of presidential protection. *The National Security Agency and Fourth Amendment Rights: Hearing on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 11 (1975) [hereinafter *Church Hearings*] (statement of Lieutenant Gen. Lew Allen, Jr., Director, NSA).

[8] *See Huston Plan Hearings*, *supra* note 7, at 1.

[9] *See id.*

[10] *See id.*; Frost, *supra* note 5. The Huston Plan was named after Deputy White House Counsel Tom Huston. *Id*.

[11] Frost, *supra* note 5.

lowed its brief existence."[12] The Church Committee would unearth FBI surveillance of private citizens and of members of antiwar and civil rights groups, including Martin Luther King, Jr.[13] The works of this committee resulted in the passage of the Foreign Intelligence Surveillance Act (FISA).

The Church Committee convened to address the Huston Plan and other unnerving intelligence community activities. One of the primary concerns expressed by Senator Mondale was the lack of Congressional guidelines that defined and controlled agencies such as the National Security Agency (NSA).[14] He noted during hearings with the director of the NSA, Lt. General Lew Allen, that only executive branch directives guided NSA operations.[15] These directives were based on policy and not law.[16] The lack of law controlling the NSA bothered Senator Mondale and led him to challenge Lt. General Allen with the following concern:

> Given another day and another President, another perceived risk and someone breathing hot down the neck of the military leader then in charge of the NSA; demanding a review based on another watch list, another wide sweep to determine whether some of the domestic dissent is really foreign based, my concern is whether that pressure could be resisted on the basis of the law or not.[17]

Senator Mondale's concern not only speaks to the motive behind the passage of FISA, but it also was predictive of the post-September 11 surveillance.[18] In the wake of the terrorist attacks on New York City and Washington, D.C., President Bush sought to increase the intelligence community's ability to prevent future attacks by Al Qaida.[19] In an effort to achieve this goal, President Bush authorized the NSA to conduct electronic surveillance on hundreds, maybe thousands, of Americans without employing the traditional warrant process or the congressionally created foreign intelligence warrant mechanism codified by FISA—the very act that Congress passed in 1978 after the

---

[12] *Huston Plan Hearings*, *supra* note 7, at 1–2 (statement of Sen. Frank Church); *see also* Frost, *supra* note 5. The Church Committee received its name from Senator Frank Church of Idaho who chaired the select committee. *Church Hearings*, *supra* note 7, at ii.

[13] *See* S. COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94–755, bk. 2, at 7 (1976); Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 103 (2006); Walter F. Mondale, *Keeping Faith in the Rule of Law*, 63 BENCH & BAR OF MINN. 26 (2006).

[14] *See Church Hearings*, *supra* note 7, at 35–36 (statement by Sen. Walter Mondale, Member, S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities).

[15] *Id.* at 36.

[16] *Id.*

[17] *See id.*

[18] *See id.*; Risen & Lichtblau, *supra* note 6.

[19] *See* Dec. 19, 2005 Press Conference, *supra* note 3, at 1885.

Watergate Scandal unearthed President Nixon's illicit NSA surveillance.[20] The full details of President Bush's 2002 authorization for electronic surveillance of Americans remain to be disclosed, but the surreptitious nature of surveillance, the targeting of American citizens, and the apparent disregard for Fourth Amendment principles are known and draw undeniable similarities to actions by President Nixon.[21] It is interesting to note that Article II of the Articles of Impeachment of Richard M. Nixon specifically states:

> He Misused the Federal Bureau of Investigation, the Secret Service, and Other Executive Personnel, in Violation or Disregard of the Constitutional Rights of Citizens, by Directing or Authorizing Such Agencies or Personnel to Conduct or Continue Electronic Surveillance or Other Investigations for Purposes Unrelated to National Security, the Enforcement of Laws, or Any Other Lawful Function of His Office; He Did Direct, Authorize, or Permit the Use of Information Obtained Thereby for Purposes Unrelated to National Security, the Enforcement of Laws or Any Other Lawful Function of His Office; and He Did Direct the Concealment of Certain Records Made by the Federal Bureau of Investigation of Electronic Surveillance.[22]

Interestingly, the Bush administration does not directly refute the accuracy or appropriateness of the analogy to President Nixon's activities.[23] Instead, the Bush administration argues that nearly every applicable Fourth Amendment and presidential power theory supports the permissibility of the program.[24] Specifically, President Bush argues that the Constitution grants the President the inherent power to conduct the electronic surveillance at issue.[25] In addition, he argues that Congress affirmed this

---

[20] *See* Risen & Lichtblau, *supra* note 6.

[21] *See id.*

[22] H.R. JUDICIARY COMM., IMPEACHMENT OF RICHARD M. NIXON, PRESIDENT OF THE UNITED STATES, H.R. REP. NO. 93–1305, art. 2, § 2, at 146 (1974) (The articles of impeachment were never voted on by the entire House of Representatives due to Richard Nixon's resignation).

[23] In response to a question that asked how the activities sanctioned by President Nixon differed from the current NSA surveillance, President Bush first refused to draw a distinction, stating instead that Presidents have this power in wartime. Only after this comment did President Bush argue that Congress had given implicit support and authority through the Authorization for Use of Military Force joint resolution in 2001. *See* Jan. 26, 2006 Press Conference, *supra* note 4, at 131. It should be noted, however, that not all Bush administration lawyers agreed with this surveillance. In fact, many lawyers, including the former Deputy Attorney General James Comey, vigorously opposed the NSA surveillance. Daniel Klaidman et al., *Palace Revolt*, NEWSWEEK, Feb. 6, 2006, at 35.

[24] *See generally* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006) [hereinafter DOJ WHITE PAPER].

[25] *Id.* at 6–10.

power through the passage of the joint resolution authorizing force in Afghanistan following the September 11 terrorist attacks.[26] Finally, he argues that the manner and method of the warrantless surveillance comports with both the requirements of FISA and the demands of the Fourth Amendment.[27]

This Article discusses why each of the arguments put forth by the Bush administration fails to justify the warrantless surveillance under both statutory and constitutional demands.[28] Part I explores the function and capabilities of the NSA, and why those capabilities are a cause for concern.[29] Part II discusses the relationship between FISA and Congress's regulation of electronic surveillance for domestic crime control through Title III[30] and provides a brief description of the key aspects of the FISA court order process and its three major exceptions.[31] Part III explains the authority granted by the Authorization for Use of Military Force passed by Congress in 2001 through a joint resolution,[32] as well as the subsequent amendments to FISA.[33] Part IV argues that the NSA surveillance program is constitutionally impermissible under FISA's statutory framework because the President has no relevant constitutional power to authorize warrantless surveillance.[34] Finally, Part V argues that the NSA surveillance program violates the Fourth Amendment.[35]

I. THE FUNCTION AND CAPABILITIES OF THE NATIONAL SECURITY AGENCY

At the core of the recent electronic surveillance controversy is the NSA—a large, secretive, and powerful agency. President Truman's initial establishment of the agency in 1952, its subsequent operations, and even its modern capabilities exist under a shroud of secrecy once so thick that the organization's nickname became "No Such Agency."[36] The NSA maintained and managed a large infrastructure footprint, but its legal authority remained scarce.[37] No congressional statute created the

---

[26] *Id.* at 10–13.

[27] *Id.* at 17–28, 36–41.

[28] It should be noted that this article is only addressing the NSA program that involved listening to international calls and reading international e-mails, not the program involving the obtaining of domestic phone records.

[29] *See infra* notes 36–94 and accompanying text.

[30] *See infra* notes 95–115 and accompanying text.

[31] *See infra* notes 116–72 and accompanying text.

[32] *See infra* notes 173–215 and accompanying text.

[33] *See infra* notes 216–44 and accompanying text.

[34] *See infra* notes 245–382 and accompanying text.

[35] *See infra* notes 383–480 and accompanying text.

[36] *See* JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY 1, 281 (1982); Risen & Lichtblau, *supra* note 6. Senator Church noted during the Church Committee Hearings in 1975 that the NSA remained unknown to most Americans at that time, both in name and in acronym. *Church Hearings*, *supra* note 7, at 1.

[37] *See Church Hearings*, *supra* note 7, at 1.

NSA or restricted its permissible scope of activities.[38] Instead, the agency was born from executive directives—directives vague in their delegation of authority and in their definition of the type of information permissible for the agency to collect.[39]

Under this secrecy, the NSA operated and operates the nation's largest intelligence agency, subsuming a large share of the estimated $40 billion budgeted annually to the intelligence community.[40] The NSA's role in the intelligence community is as the primary collector of signals intelligence (SIGINT).[41] SIGINT is a catchall term that includes all intelligence derived from communications, as well as from electronic and instrumentation emissions.[42] The NSA collects this information through highly technological sensors, including listening posts, satellites, and satellite dishes.[43] For instance, the NSA maintains over twenty satellite dishes alone in Menwith Hill, England.[44] The NSA integrates these sensors into a global spy system often referred to as ECHELON, which is maintained with the cooperation and contribution of England, Canada, Australia, and New Zealand.[45] Former Congressman Bob Barr described ECHELON as the equivalent of a global vacuum cleaner that sucks up signal intelligence from all over the world and then provides this information to intelligence analysts to exploit.[46]

The result of this global surveillance network is a massive amount of raw intelligence, including virtually every electronic conversation around the world.[47] This information is generally sifted through by data mining techniques that register particular

---

[38] *Id.*

[39] *Id.*

[40] David Ensor, *Brave New World: Agency's Challenges More Complex in Post-Cold War Era*, CNN.COM, Mar. 19, 2001, http://www.cnn.com/SPECIALS/2001/nsa/stories/codebreakers/index.html; FAS.org, Tracing the Rise and Fall of Intelligence Spending, http://www.fas.org/irp/budget/index.html (last visited Nov. 21, 2006).

[41] *See* U.S. Dep't of Defense, Directive No. 5100.20, ¶ 2.2 (Dec. 23, 1971) (as amended through June 24, 1991), *available at* http://www.dtic.mil/whs/directives/corres/pdf2/d510020p.pdf [hereinafter Directive No. 5100.20]; FAS.org, SIGINT Overview, Mar. 9, 1997, http://www.fas.org/spp/military/program/sigint/overview.htm.

[42] *See* Directive No. 5100.20, *supra* note 41, ¶ 3.1.

[43] *See* Ensor, *supra* note 40.

[44] *Id.* The U.S. Army Security Agency initially operated Menwith Hill Station when it officially, though secretly, opened on September 15, 1960. *See* BAMFORD, *supra* note 36, at 208. The base provided an environment free from urban electromagnetic interference, which made it ideal for electronic surveillance. *Id.* at 209. The NSA took over the operations of Menwith Hill on August 1, 1966. *Id.*

[45] *60 Minutes: ECHELON; Worldwide Conversations Being Received* (CBS television broadcast Feb. 27, 2000) [hereinafter *60 Minutes*], *available at* http://www.freerepublic.com/focus/f-news/1543347/posts.

[46] Douglas C. McNabb & Matthew R. McNabb, *Of Bugs, the President, and the NSA: National Security Agency Intercepts Within the United States*, THE CHAMPION, Mar. 2006, at 10, 15.

[47] *See id.*

words, phrases, or voices.[48] The NSA collects this information for analysis by tactical and strategic military leaders, policymakers, and other intelligence agencies.[49]

For much of its history, the immense capabilities and collection framework of the NSA were limited to targeting foreign powers and organizations.[50] The Bush administration changed that scope by allowing the NSA to conduct warrantless electronic surveillance on persons in the United States.[51] No longer would the NSA restrict its warrantless actions to foreign to foreign terminal communications, but it would now include information originating from or going to a domestic terminal.[52] *The New York Times*, in the article that broke this issue to the public, estimates that the NSA eavesdrops on an estimated 500 persons in the United States at any given time.[53] President Bush, so as to alleviate the fears stressed in reference to the intercepted calls, stated, "They are from outside the country to in the country or vice versa. So in other words, . . . if you're calling from Houston to L.A., that call is not monitored."[54] The inclusion of any domestic terminal, however, is the crux of the concern expressed by the public, the legal profession, and Congress.

During the 1970s, similar concerns about the capabilities and the expanding power of the NSA were expressed by both Congress and the Supreme Court.[55] Senator Church noted the constitutional and civil liberties concerns during the 1975 congressional hearings regarding abuse of power by the NSA stating that "[t]he danger lies in the ability of the NSA to turn its awesome technology against domestic communications."[56]

The warrantless NSA surveillance authorized by President Bush has already shown signs of the gradual expansion that generally follows the employment of such collection programs.[57] The program initially sought to exploit the telephone numbers and e-mail

---

[48] *See* Walter Pincus, *NSA Gave Other U.S. Agencies Information from Surveillance*, WASH. POST, Jan. 1, 2006, at A8.

[49] *See* Nat'l Sec. Agency, Signals Intelligence, http://www.nsa.gov/sigint/index.cfm (last visited Aug. 27, 2006) [hereinafter Signals Intelligence].

[50] Signals Intelligence, *supra* note 49; Risen & Lichtblau, *supra* note 6.

[51] *See* Risen & Lichtblau, *supra* note 6.

[52] *See id.*

[53] *Id.*

[54] Dec. 19, 2005 Press Conference, *supra* note 3, at 1889.

[55] *See, e.g.*, United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 312–13 (1972) ("There is, understandably, a deep-seated uneasiness and apprehension that this capability [electronic surveillance] will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy."); *Church Hearings*, *supra* note 7, at 10–13, 30 (statement of Lieutenant Gen. Lew Allen, Jr.) (describing the mission creep associated with the NSA collection program, Operation MINARET).

[56] *Church Hearings*, *supra* note 7, at 2.

[57] *See* Risen & Lichtblau, *supra* note 6. Such undue expansion can also occur from an effort to be *more discriminatory* in the use of surveillance. For example, in Operation MINARET, discussed *infra* at notes 79–86 and accompanying text, the NSA sought to amplify its target selection by including a target's address or potential aliases. Though this process sought great precision in the identification of a target, the result was the collection

addresses from Al Qaida operatives captured in Afghanistan.[58] It naturally expanded to include individuals linked more and more tenuously with the originally identified targets.[59] While mere speculation, it will be interesting to see whether this program expanded even further to include members of protest groups in the United States or to target individuals in support of the military operation in Iraq.

The concerns associated with the NSA surveillance are not limited to institutional apprehension, but they are closely linked to a history of abuse of this technology during the Cold War period.[60] The activities and abuses by the NSA rose to public consciousness during the 1970s, specifically as a result of the Watergate scandal and the resulting congressional hearings. The particular nature of the abuses are most appropriately understood through judicial efforts to address those activities in the Supreme Court case of *United States v. United States District Court* (*Keith*) and through congressional efforts evidenced by the Church Committee Hearings in 1975.[61]

The Supreme Court, in 1972, sought to curb executive branch discretion to employ national security wiretaps to further domestic security.[62] In the *Keith* case, the Supreme Court faced the question of whether the President could authorize electronic surveillance without prior judicial approval in domestic security matters.[63] The wiretaps at issue were justified with the purpose "to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."[64] The government sought to use information gathered by this surveillance in the prosecution of three defendants charged with the bombing of a CIA office in Michigan.[65]

The government argued that the President's national security power made the surveillance lawful, despite its warrantless nature.[66] The Supreme Court began its analysis by noting that Article II of the United States Constitution provides the President with the power and duty to protect against those who would plot against the

---

and use of more information. *See Church Hearings*, *supra* note 7, at 13 (statement of Lieutenant Gen. Lew Allen, Jr.).

[58] Risen & Lichtblau, *supra* note 6 (detailing the original intent to exploit the information contained in computers, cellphones, and personal phone directories of Al Qaida operatives, including Abu Zubaydah, captured by the CIA in Afghanistan and Pakistan).

[59] *See id.* (describing how the chain of connections quickly expanded).

[60] *See Keith*, 407 U.S. at 324 (holding the use of electronic surveillance for domestic security without prior judicial approval unlawful); *Church Hearings*, *supra* note 7, at 2 (detailing the need for congressional hearings to address the abuse of power by the NSA).

[61] 407 U.S. 297. *See generally Church Hearings*, *supra* note 7.

[62] *See Keith*, 407 U.S. at 316–18 ("These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.").

[63] *Id.* at 299.

[64] *Id.* at 300.

[65] *Id.* at 299.

[66] *Id.* at 301.

government.[67] The national security justification, however, is wrought with constitutional problems, especially when "the Government attempts to act under so vague a concept as the power to protect 'domestic security'" due to the difficulty of defining the imperative interest.[68] The Court raised the concern that the discretion to conduct the electronic surveillance rested solely within the executive branch, disabling the officers in charge from constituting the neutral and disinterested judiciary contemplated by the Fourth Amendment.[69] In addition, the Court rejected the government's arguments that practical circumstances foreclosed the ability to obtain a warrant and that internal security matters are too complex and subtle for the courts to evaluate.[70]

Thus, the Supreme Court held that warrantless domestic electronic surveillance, even when justified by national security imperatives, must comply with traditional Fourth Amendment standards.[71] The Court went on to invite Congress to consider protective standards for domestic security contexts in a manner similar to the standards that were specifically detailed in congressional regulation of electronic surveillance for ordinary crime.[72] Congress responded to this invitation, in part, by debating the appropriate protective standards during the Church Committee Hearings.[73]

Congress conducted extensive hearings into presidential abuse of power during the Watergate scandal.[74] At the Watergate Hearings, Congress and the public were first exposed to the vast and unregulated nature of the nation's intelligence agencies but particularly to the National Security Agency.[75] Congress acted upon these revelations and public outcry by holding public and executive session hearings to understand and expose the nature of the NSA's activities.[76] This Congressional inquiry would be later called the Church Committee Hearings and would serve the self-labeled purpose of bringing "the Agency from behind closed doors."[77]

Senator Church and the other members of the select committee conducted much of the hearings in closed, executive session, but the public hearings present a substantive view of the illicit surveillance conducted by the NSA.[78] Information on two

---

[67] *Id.* at 310.

[68] *Id.* at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power.").

[69] *See id.* at 316–17.

[70] *See id.* at 320.

[71] *See id.* at 320–21.

[72] *See id.* at 322–23; Omnibus Crime Control and Safe Streets (Title III) Act of 1968, Pub. L. No. 90–351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (2000 & Supp. III 2003)) (providing protective standards applicable to electronic surveillance for general crime control).

[73] *See generally Church Hearings*, *supra* note 7.

[74] *See* BAMFORD, *supra* note 36, at 289–90.

[75] *See id.*

[76] *See generally Church Hearings*, *supra* note 7.

[77] *Church Hearings*, *supra* note 7, at 1 (statement of Sen. Frank Church).

[78] *See, e.g.*, *id.* at 30, 57–58 (detailing secret surveillance programs Operation MINARET and Operation SHAMROCK).

previously classified programs, Operation MINARET and Operation SHAMROCK, was approved for public dissemination, and those programs provide an illuminating view of what FISA sought to prevent from occurring in the future.[79]

Operation MINARET officially began in 1969. It formalized the process that began in 1967 to utilize the NSA to intercept communications in order to determine the existence of foreign influence on civil disturbances occurring in the United States related to the Vietnam War and to assist in presidential protection.[80] During the period between its inception and its subsequent discovery and termination in 1973, the emphasis of the NSA surveillance soon expanded to include international drug trafficking and acts of terrorism.[81]

In practice, MINARET constituted a "watch list" of activity whereby the NSA sorted through the electronic communication captured by identifying particular words, names, subjects, and locations.[82] The problematic nature of MINARET entailed the placement of American citizens and organizations on the watch list.[83] During MINARET's operational years, the watch lists contained roughly 1,650 names of United States citizens, with up to 800 names on the list at any given time.[84] The operation internally justified the activity not only based upon the national security need for the information, but also because it expanded the term "foreign intelligence" to require only one foreign terminal from which the communications originated.[85] It was, however, this ability to define foreign intelligence to include domestic terminals and persons that led to congressional criticism.[86]

The second clandestine program that the Church Committee unearthed and exposed to the public was codenamed Operation SHAMROCK.[87] SHAMROCK entailed a message-collection program whereby the NSA tasked private international telegraph

---

[79] *See id.*

[80] *See id.* at 10–11, 30 (statement of Lieutenant Gen. Lew Allen, Jr.). Indications exist that this surveillance began even earlier in the 1960s to monitor United States citizens traveling to Cuba. *See id.* at 10. This concern likely dovetailed with concerns at the time that the assassination of President Kennedy resulted from Cuban retaliation for attempts against the life of Fidel Castro. *See* S. COMM. ON ASSASSINATIONS, H.R. REP. NO. 95–1828, pt. 2, at 109–14 (1979). The 1969 charter for MINARET was to provide for "more restrictive control and security of sensitive information derived from communications" and "specifically include[d] communications concerning individuals or organizations involved in civil disturbances, anti-war movements/demonstrations and military deserters involved in anti-war movements." *Id.* at 150 (Exhibit 3: July 1, 1969 Memo from an Assistant Director, NSA).

[81] *Church Hearings*, *supra* note 7, at 11 (statement of Lieutenant Gen. Lew Allen, Jr.).

[82] *Id.* at 10.

[83] *See id.* The problematic nature of Operation MINARET became even more apparent after the Supreme Court's decision in *Keith* described *supra* in notes 61–72. *See* BAMFORD, *supra* note 36, at 292.

[84] *Church Hearings*, *supra* note 7, at 12.

[85] *See id.* at 10.

[86] *See id.* at 37–38.

[87] *Id.* at 57–58.

companies to provide certain international communications to the intelligence agency.[88] This program originally began operating in 1947 under the control of the Army Security Agency, which relinquished operational control over SHAMROCK first to the Armed Forces Security Agency upon its creation in 1949 and then again to the NSA in 1952.[89]

At the outset of the program, the efforts focused on extracting only "international telegrams relat[ed] to certain foreign targets."[90] This purpose changed throughout the years to include the extraction of telegrams for certain United States citizens.[91] As with Operation MINARET, no constitutional infirmity resulted from Operation SHAMROCK while its efforts targeted foreign terminal to foreign terminal communications.[92] Operation SHAMROCK became illegal, both as a violation of the Fourth Amendment of the United States Constitution and, as argued at the Church Committee, in violation of the Communications Act of 1934, once it began to target United States citizens and domestic terminals.[93] A noteworthy and instructive element of both Operation MINARET and Operation SHAMROCK is that each program gradually and shamelessly expanded beyond its original scope and initial justification.[94]

II. THE RELATIONSHIP BETWEEN TITLE III AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

As a result of the Church Hearings, Congress felt compelled to take remedial action in terms of a comprehensive statutory framework.[95] The result was the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978.[96] FISA began, however, not as a separate act but as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[97] Title III authorized and regulated the use

---

[88] *Id.* The private companies were RCA Global, ITT World Communications, and Western Union International. *Id.* (statement of Sen. Frank Church); *see* BAMFORD, *supra* note 36, at 240–41 (describing the details of the message-collection program instituted with RCA).

[89] *Church Hearings*, *supra* note 7, at 59.

[90] *Id.* at 58.

[91] *Id.* During the 1970s, NSA subjected roughly 150,000 messages per month to further review by intelligence analysts. *Id.* at 60. *Cf.* BAMFORD, *supra* note 36, at 241 (detailing the concerns about illegality of such a program expressed by both Western Union and RCA).

[92] *See Church Hearings*, *supra* note 7, at 10, 60.

[93] *See id.* at 62 (statement of Sen. Gary Hart, Member, S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities).

[94] *See id.* at 12–13, 57–58 (statements of Lieutenant Gen. Lew Allen, Jr., and Sen. Frank Church).

[95] *See id.* at 61. Senator Goldwater, while arguing against disclosure of this information to the public, conceded that "[t]he American people expect the Congress to take remedial action when necessary." *Id.*

[96] *See* FISA, 50 U.S.C. §§ 1801–1811 (2002).

[97] *See* Title III, Pub. L. No. 90–351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (2000 & Supp. III 2003)); *see also* Memorandum from Elizabeth B. Bazan &

of electronic surveillance for criminal law enforcement purposes. It required that such surveillance be authorized by prior judicial approval and circumscribed the conditions for its use.[98] Congress intended the passage of Title III to ensure the privacy interests of domestic persons, while providing the government with the flexibility to ensure effective crime control.[99] The process and procedures provided by Title III for the Attorney General to seek a court order authorizing electronic surveillance were drafted to satisfy constitutional requirements provided by the Supreme Court in *Katz v. United States*[100] and *Berger v. New York*.[101] It should be pointed out that *Katz* included oral communications within the purview of the Fourth Amendment even if no physical trespass was required to obtain these conversations.[102]

The procedures provided by Title III sought to regulate electronic surveillance for criminal law enforcement, but they did not attempt to address electronic surveillance conducted pursuant to national security interests.[103] Title III included a proviso in the original section 2511(3) that expressed congressional neutrality on the issue of regulating the President's national security powers to conduct electronic surveillance.[104] Based on that proviso and the general purpose of Title III, the Supreme Court, in *Keith*, stated that the act did "not attempt to define or delineate the powers of the President to meet domestic threats to the national security."[105]

The Supreme Court in *Keith* also recognized that different protective schemes may be required when distinguishing between efforts to conduct general criminal surveillance and those that involve domestic security.[106] Congress would accept this invitation to provide a separate but integrated protective scheme for electronic surveillance driven by national security interests with the passage of FISA.[107] In passing

---

Jennifer K. Elsea, Legislative Attorneys, Am. Law Div., Cong. Res. Serv., 14–17 (Jan. 5. 2006) [hereinafter Bazan & Elsea], *available at* http://www.fas.org/sgp/crs/intel/m010506.pdf (providing a general framework and analysis for the constitutional and statutory arguments that the President has employed to justify the NSA electronic surveillance).

[98] United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 301–02 (1972); Bazan & Elsea, *supra* note 97, at 14.

[99] *See Keith*, 407 U.S. at 302.

[100] 389 U.S. 347 (1967).

[101] 388 U.S. 41 (1967) (holding that the use of electronic devices to hear conversations constituted a search under the Fourth Amendment); *see Keith*, 407 U.S. at 102; Bazan & Elsea, *supra* note 97, at 8. *See generally Katz*, 389 U.S. 347 (holding that the Fourth Amendment applies to recording oral statements).

[102] *Katz*, 389 U.S. at 352–53.

[103] *See Keith*, 407 U.S. at 308.

[104] *See id.* at 302–03. The insertion of this proviso was orchestrated, at least in part, by Roy Banner, a top lawyer at the NSA. BAMFORD, *supra* note 36, at 256. Banner helped draft this loophole to provide the legal cover for the NSA's domestic signal intelligence. *Id.*

[105] *Keith*, 407 U.S. at 322.

[106] *Id.* at 322–23 ("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.").

[107] *See* Bazan & Elsea, *supra* note 97, at 17–18. *See generally* FISA, 50 U.S.C. §§

FISA, Congress carved a separate legal regime from Title III to address and govern the collection of "foreign intelligence" through electronic surveillance methods.[108] Title III remains to govern ordinary criminal law enforcement purposes.[109] Congress in enacting FISA sought to "provide the secure framework by which the executive branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights."[110]

The different protective schemes for the use of electronic surveillance provided in Title III and FISA demonstrate the different balancing of the governmental interest against the resulting privacy intrusion on an individual.[111] Specifically, under Title III, the Attorney General or an authorized representative must apply for a court order approving the electronic surveillance through a process similar to a search warrant.[112] The statute strictly prohibits nearly all electronic surveillance conducted outside of the court authorization detailed in section 2516.[113] FISA does not provide for any wide-ranging exceptions for non-authorized surveillance, but three statutorily circumscribed exceptions exist and are described below.[114]

The comparison and relationship between the protective schemes provided in Title III and those provided in FISA are illuminating because they show: (1) broad, if not exclusive, congressional regulation in the sphere of electronic surveillance; (2) specific congressional intent for FISA to govern foreign intelligence surveillance as distinct from general criminal law enforcement; and (3) the provision of a more relaxed protective standard and application process to allow the executive branch to address the national security need for foreign intelligence collection through a congressionally authorized statutory scheme.[115]

A. Statutory Framework of the Foreign Intelligence Surveillance Act (FISA)

The protective scheme designed by Congress for the collection of foreign intelligence sought to recognize and address the government's legitimate need to collect

---

1801–1811 (2002).

[108] Bazan & Elsea, *supra* note 97, at 17–18.

[109] *Id.* at 14.

[110] S. REP. NO. 95–604, pt. 1, at 15 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3916.

[111] *See* Bazan & Elsea, *supra* note 97, at 18 (detailing the relaxed probable cause standard in FISA compared with the more traditional probable cause requirement in Title III).

[112] *See* Title III, 18 U.S.C. §§ 2516, 2518 (2000 & Supp. III 2003).

[113] *See id.* § 2511. Section 2511(1) applies a civil penalty to any person who "intentionally intercepts," "intentionally uses," or "intentionally discloses" electronic communications except for narrow exceptions such as when the person has been authorized by a separate federal statute (e.g., FISA). *Id.* § 2511(1)(a)–(e).

[114] *See infra* notes 147–72 and accompanying text.

[115] *See* S. REP. NO. 95–604, at 6, 1978 U.S.C.C.A.N. at 3907 (describing the intent of Congress for FISA and Title III to constitute the exclusive means by which domestic electronic surveillance may be conducted); David Cole et al., *On NSA Spying: A Letter to Congress*, N.Y. REVIEW OF BOOKS, Feb. 9, 2006, at 42; Bazan & Elsea, *supra* note 97, at 14.

such intelligence, while also providing a method for judicial intervention to protect against invasions into the privacy interests of individuals unearthed during the Church Committee Hearings.[116]

In order to effectuate this delicate balancing between the important government interest and the protection of individual privacy, Congress designed and implemented a special court that would provide both the expediency and secrecy needed to address foreign intelligence concerns, while retaining the important protection of placing a neutral judicial representative between the government enforcement officials—the intelligence community as represented by the Attorney General—and the people or places targeted for surveillance.[117] The United States Foreign Intelligence Surveillance Court (FISC) and the United States Foreign Intelligence Surveillance Court of Review (Court of Review) were constituted to serve this purpose.[118] The composition of the FISC originally included "seven U.S. district court judges publicly designated by the Chief Justice of the United States Supreme Court."[119] Three U.S. district court or U.S. court of appeals judges, again publicly designated by the Chief Justice, constituted and still constitute the Court of Review.[120]

Congress designed this special court system to review executive branch applications for electronic surveillance aimed at obtaining foreign intelligence.[121] This application process sought to mirror the traditional law enforcement warrant process to the extent that national security exigency and practicality would allow.[122] This congressionally preferred application process also envisions situations when, similar to the traditional warrant process, the exigency of the situation demands a deviation from the more formal procedure.[123] To accommodate these special circumstances, FISA includes three exceptions that provide additional latitude for the executive branch.[124] The first exception allows for surveillance without a court order when the

---

[116] *See* S. REP. NO. 95–604, at 7–8, 1978 U.S.C.C.A.N. at 3908–09 ("[This bill] goes a long way in striking a fair and just balance between protection of national security and protection of personal liberties.").

[117] *See* ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND RECENT JUDICIAL DECISIONS 8–16 (CONG. RES. SERV. 2005), *available at* http://www.fas.org/sgp/crs/intel/RL30465.pdf.

[118] *See id.* at 2 n.6.

[119] *Id.* The USA PATRIOT Act increased the FISC to eleven district court judges, at least three of whom must live within a twenty-mile radius of the District of Columbia. 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, § 208, 115 Stat. 272, 283 (2001) (codified at 50 U.S.C. § 1803 (2000 & Supp. III 2003)).

[120] BAZAN, *supra* note 117, at 2 n.6.

[121] *See* S. REP. NO. 95–604, at 5, 1978 U.S.C.C.A.N. at 3907.

[122] *See id.* at 5–6, 1978 U.S.C.C.A.N. at 3906–07 (recognizing that exigent circumstances may require a limited departure from the congressionally preferred judicial application and approval process).

[123] *See id.*

[124] *See* FISA, 50 U.S.C. §§ 1802, 1805(f), 1811.

targets are solely foreign governmental entities because of the lesser privacy interests at stake.[125] The second and third exceptions allow for surveillance with only retrospective FISC review because the national security imperative renders immediate surveillance necessary and the traditional court order process impracticable.[126] Finally, if the FISC denies the application for electronic surveillance, FISA provides two layers of judicial review, with appeal first to the Court of Review and second to the United States Supreme Court.[127]

The FISC order process differs from the traditional warrant process as it provides greater deference to the executive branch through relaxed application standards.[128] After an application is made, a FISC judge *must* issue a warrant if: (1) the President has authorized the Attorney General to approve applications for such electronic surveillance;[129] (2) the application has been approved by the Attorney General;[130] (3) on the basis of facts submitted to the court, probable cause exists to believe the target of the surveillance is a foreign power or an agent of a foreign power and that the place at which the surveillance is directed is being used or about to be used by that foreign power or agent;[131] (4) the minimization procedures (minimization) seek to limit acquisition, retention, and dissemination;[132] and (5) if the target is a United States person,

---

[125] *See id.* § 1802; S. REP. NO. 95–604, at 50, 1978 U.S.C.C.A.N. at 3951–52.

[126] *See* FISA, 50 U.S.C. §§ 1805(f), 1811; S. REP. NO. 95–604, at 51–52, 1978 U.S.C.C.A.N. at 3953; H.R. REP. NO. 95–1720, at 34 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4063. For a further discussion of these exceptions, see *infra* notes 147–72 and accompanying text.

[127] S. REP. NO. 95–604, at 5, 1978 U.S.C.C.A.N. at 3906 (detailing the intent to provide two layers of appeal for the government after a denial of a FISA warrant by the FISC).

[128] *See, e.g.*, Bazan & Elsea, *supra* note 97, at 18, 23–26 (detailing FISA's relaxed probable cause standard and the major exceptions designed to provide limited executive branch electronic surveillance based on exigent circumstances).

[129] This requirement is largely formalistic, but its purpose is consistent with Congress's desire to provide an internal check by requiring written accountability within the executive branch for the decision to engage in electronic surveillance. *See* S. REP. NO. 95–604, at 48–49, 1978 U.S.C.C.A.N. at 3950.

[130] The Attorney General's certification must be in writing to serve the internal check function, and it must attest to the satisfaction of the statutory requirements for the application detailed in § 1804 and that, under his or her belief, probable cause exists. FISA, 50 U.S.C. § 1805(a)(2); S. REP. NO. 95–604, at 43–44, 1978 U.S.C.C.A.N. at 3945. The statutory requirements for the application are set forth in § 1804. FISA, 50 U.S.C. § 1804(a). The requirement that the Attorney General, Acting Attorney General, or Deputy Attorney General personally approve the application was intended to provide a bulwark against high-ranking official pressure from the heads of agencies such as the Central Intelligence Agency or the Federal Bureau of Investigation. *See* S. REP. NO. 95–604, at 36, 1978 U.S.C.C.A.N. at 3937–38.

[131] The requirement for probable cause is discussed further *infra* at notes 139–46 and accompanying text.

[132] The flexibility given to the executive branch in the FISA requirements is intended to be offset by the requirement for reasonable minimization procedures. These procedures are designed to restrict the information obtained concerning United States persons through electronic surveillance to foreign intelligence pursuant to a general policy of limiting the acquisition, retention, and

the certification is not clearly erroneous.[133] Congress intended through this framework to provide a scheme of internal checks within the executive branch and external checks with the interjection of review by a neutral judge to curb arbitrary executive action.[134]

The deference provided to the executive branch in this process is evident from the limited, ministerial judicial review by the FISC judge and the relaxed probable cause standard. First, when the executive branch satisfies the application requirements, the FISC judge *must* issue the FISA warrant.[135] The FISC judge is not permitted to substitute his or her judgment for that of the executive branch and has no authority to "look behind" the application.[136] The one exception to this lack of discretion occurs when the surveillance targets a United States person.[137] "In such a case, the judge must review the certifications to determine whether they are clearly erroneous."[138]

The second area of deference to the executive involves the requirement of probable cause.[139] The probable cause requirement in Title III closely tracks the traditional probable cause requirement and necessitates a showing that the "target has committed, is committing, or is about to commit a crime."[140] FISA, however, requires only that the

---

dissemination of information. *See* S. REP. NO. 95–604, at 54–55, 1978 U.S.C.C.A.N. at 3956; S. REP. NO. 95–701, at 41 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 4010. Congress recognized that the best practice to accomplish this goal is to encourage the destruction of information that provides no foreign intelligence information. S. REP. NO. 95–701, at 42, 1978 U.S.C.C.A.N. at 4011. The definition of "minimization procedures" requires a course of action "reasonably designed" in relation to the specific purpose of the electronic surveillance requested. FISA, 50 U.S.C. § 1801(h)(1). The specific procedures required, therefore, are fact-specific and may depend upon the scope of the enterprise under investigation, the location and operation of the target, the government's expectations of the character of the parties and calls, and the length of the surveillance. S. REP. NO. 95–604, at 37–38, 1978 U.S.C.C.A.N. at 3939. The Attorney General must provide a statement of the proposed minimization procedures and the FISC judge will review the statements for their reasonableness. FISA, 50 U.S.C. §§ 1804(a)(5), 1805(a)(4).

[133] The "clearly erroneous" standard is discussed further *infra* notes 137–38 and accompanying text. For the necessary findings required before issuance of a FISA warrant, see FISA, 50 U.S.C. § 1805(a).

[134] *See* S. REP. NO. 95–604, at 48–49, 1978 U.S.C.C.A.N. at 3950.

[135] FISA, 50 U.S.C. § 1805(a) ("Upon an application made pursuant to section 1804 of this title, the judge *shall* enter an ex parte order . . . .") (emphasis added); *see* S. REP. NO. 95–604, at 48–49, 1978 U.S.C.C.A.N. at 3950.

[136] *See* S. REP. NO. 95–604, at 48, 1978 U.S.C.C.A.N. at 3950. Though this may appear to present a rubber stamp procedure, the purpose is to assure written accountability within the executive branch for the decision to engage in electronic surveillance, thus providing an internal check against arbitrariness. *Id.* at 48–49, 1978 U.S.C.C.A.N. at 3950.

[137] *Id.* at 48, 1978 U.S.C.C.A.N. at 3950.

[138] *Id.* The "clearly erroneous" standard was intended to be less strict than a finding of probable cause. *Id.*

[139] *See* Bazan & Elsea, *supra* note 97, at 18.

[140] *Id.*; *see* Draper v. United States, 358 U.S. 307, 313 (1959) (defining probable cause for general law enforcement as "where 'the facts and circumstances within [the arresting officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or

target of the electronic surveillance be a foreign power or an agent of a foreign power and that each of the places targeted is or will be used by a foreign power or agent of a foreign power.[141] As a result, the standard for probable cause in the FISA context is not as strict as for general crime control.[142] FISA does not require a finding that a crime is imminent or that the elements of a specific crime exist, but it requires instead a more speculative standard that allows surveillance to occur at an earlier stage in the investigative process.[143] This speculative standard is evidenced in the agency-based definition for an "agent of a foreign power."[144] A person may satisfy this statutory definition, and thus satisfy the probable cause requirement, when a person "knowingly engages" or "may involve" oneself in subversive activities.[145] In addition, the FISC judge must make this determination based upon the facts and circumstances provided by the executive branch.[146] The probable cause requirement, therefore, defers greatly to the executive branch to allow it to determine when probable cause exists and then to provide the FISC judge only limited discretion to challenge such a determination.

B. Exceptions to the Congressionally Preferred Court Order Process

In addition to the deference and flexibility that Congress gave to the executive branch for obtaining a judicial order authorizing electronic surveillance, Congress also contemplated three scenarios when the exigencies of national security needs could require limited surveillance without a FISC order.[147] Each of these scenarios defers in favor of the national security imperatives when balancing the need for adequate intelligence against the preservation of privacy rights.[148] Congress sought, however, to limit these exceptions to court-ordered electronic surveillance by restricting the target and duration, as well as imposing additional procedural safeguards.[149]

---

is being committed." (citing Carroll v. United States, 267 U.S. 132, 162 (1925))).

[141] FISA, 50 U.S.C. § 1805(a)(3) (2002); *see* Bazan & Elsea, *supra* note 97, at 18. The six groups or entities that constitute a "foreign power" and the groups or individuals that represent an "agent of a foreign power" are defined in § 1801. FISA, 50 U.S.C. § 1801(a)–(b).

[142] *See* S. REP. NO. 95–701, at 11–13 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3980–81.

[143] *See id.*

[144] *See* FISA, 50 U.S.C. § 1801(b).

[145] FISA, 50 U.S.C. § 1801(b)(2)(A).

[146] *See* FISA, 50 U.S.C. § 1805(a)(3).

[147] FISA, 50 U.S.C. §§ 1802(a)(1) (electronic surveillance of communications exclusively between or among foreign powers for up to one year), 1805(f) (emergency orders for up to seventy-two hours), 1811 (wartime exigency for up to fifteen days following a congressional declaration of war).

[148] *See* S. REP. NO. 95–604, pt. 1, 1, 3–5, 50–51 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3904, 3905–06, 3952.

[149] *See* FISA, 50 U.S.C. §§ 1802(a)(1) (surveillance on foreign powers for up to one year), 1805(f) (emergency orders for up to seventy-two hours), 1811 (fifteen days after declaration of war).

The most expansive exception to court-ordered surveillance occurs when the electronic surveillance targets official foreign powers (Foreign Powers Exception).[150] Congress provided the executive branch with the ability to conduct electronic surveillance to acquire foreign intelligence for up to one year without a court order as long as the Attorney General certifies in writing to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence that the following conditions exist: (1) the target falls within an official foreign power definition, (2) there is no substantial likelihood a United States person will be a party to the communication, and (3) reasonable minimization procedures are in place.[151] The Attorney General's certification must occur at least thirty days prior to the effective date of the surveillance, unless the surveillance must occur immediately, which then requires the Attorney General to notify the committees immediately.[152] In addition, the Attorney General must, in all situations, "immediately transmit" a copy of the certification under seal to the FISC.[153]

In order for the Attorney General to authorize the surveillance, there is no requirement of judicial review or approval,[154] no need to provide a factual detail of the information sought by the electronic surveillance,[155] and no court control over the duration of the surveillance unless it exceeds one year.[156] Instead, arbitrary electronic surveillance is limited by the internal checks required to obtain the Attorney General's approval, the external checks of written justification to the FISC and the congressional committees, and the substantive check of statutory requirements.[157]

The definition of foreign powers in this exception provides the most substantive check on its scope.[158] The Foreign Powers Exception only applies to entities that are clearly "arms of a government."[159] This definition excludes the more privately-controlled entities such as terrorist groups and foreign-based political organizations, as well as the entire category of agents of a foreign power.[160]

---

[150] FISA, 50 U.S.C. § 1802(a)(1)(A).

[151] *Id.* § 1802(a)(1).

[152] *Id.*

[153] *Id.* § 1802(a)(3).

[154] Congress did intend, however, for limited judicial review of the effectiveness of the minimization procedures in order to protect United States persons from undue surveillance. *See* S. REP. NO. 95–604, pt. 1, at 51 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3952.

[155] Congress, when discussing the exception of the same official foreign powers from providing a factual description under the preferred court ordered process, stated that "the sensitivity of the surveillance is greatly multiplied while the risk of a fruitless surveillance which will not obtain any foreign intelligence information is greatly reduced." *Id.* at 45, 1978 U.S.C.C.A.N. at 3946.

[156] *Id.* at 48–50, 1978 U.S.C.C.A.N. at 3950–51.

[157] *See* FISA, 50 U.S.C. § 1802(a).

[158] *See id.* § 1801(a)–(c); S. REP. NO. 95–701, at 17 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3986.

[159] *See* S. REP. NO. 95–701, at 17, 1978 U.S.C.C.A.N. at 3986.

[160] *See* FISA, 50 U.S.C. § 1802(a)(1)(A) (partially incorporating the definition of foreign power in § 1801(a)); § 1801(a)(1)–(3); *cf.* § 1801(a)(4)–(6).

This substantive restriction not only limits the exception but justifies it. The inclusion of this exception amended the original Senate bill and provoked widespread criticism among the Senate Judiciary Committee.[161] The Ford administration argued for the exception and justified it on three grounds: (1) the determination that an entity fits one of the three special classes of foreign powers "is not likely to be erroneous," (2) "the likelihood of obtaining valuable foreign intelligence" from these targets is high, and (3) such surveillance is likely required for longer periods of time.[162]

Congress also contemplated that the need for electronic surveillance could occur during an emergency when obtaining a court order would be impossible before the surveillance should begin.[163] In such a situation, Congress intended to place the Attorney General in the role of the FISC during the emergency period until judicial review could be obtained.[164]

The limits on this exception include the expiration of authorization for such electronic surveillance after seventy-two hours or when the information sought is obtained.[165] In addition, the following requirements must also be satisfied: (1) the factual basis exists under the general FISA requirements to support the surveillance; (2) a FISA judge must be immediately notified of the emergency surveillance, (3) an application pursuant to the preferred method of authorization must be processed as soon as practicable,[166] and (4) minimization procedures must still be followed.[167] This exception also incorporates an exclusionary provision that prevents information gathered through this exception to be used in a judicial proceeding unless the FISC issued a court order approving the surveillance.[168] The limits placed on this exception balance the need to provide the executive branch with the flexibility to respond to immediate, emergency national security needs within a framework that retains the external checks of judicial review.[169]

---

[161] S. REP. NO. 95–604, at 50, 1978 U.S.C.C.A.N. at 3951–52.

[162] *Id.*

[163] FISA, 50 U.S.C. § 1805(f).

[164] S. REP. NO. 95–604, at 52, 1978 U.S.C.C.A.N. at 3953.

[165] FISA, 50 U.S.C. § 1805(f).

[166] *Id.* This application must be made even if the surveillance is terminated before the twenty-four hour emergency period expires. *See* S. REP. NO. 95–604, at 52, 1978 U.S.C.C.A.N. at 3953.

[167] FISA, 50 U.S.C. § 1805(f).

[168] *Id.* ("In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.").

[169] *See* S. REP. NO. 95–604, at 51–52, 1978 U.S.C.C.A.N. at 3953.

The final exception allows the Attorney General to authorize electronic surveillance without a court order in a time of war.[170] This authorization expires after fifteen days and requires a preceding declaration of war by Congress.[171] Congress intended this exception to provide a limited time period in which the President could conduct electronic surveillance without a court order while Congress considered whether any amendments to FISA were required to address the new wartime scenario.[172]

III. THE SCOPE OF AUTHORITY GRANTED BY THE AUTHORIZATION FOR USE OF MILITARY FORCE

The Bush administration makes three principle and mutually independent arguments in an effort to defend the legality of the warrantless electronic surveillance program.[173] Specifically, the administration argues that: (1) the surveillance program satisfies the statutory requirements of FISA;[174] (2) the President retains inherent and exclusive authority to conduct such an electronic surveillance program;[175] and (3) even if the President does not have exclusive authority, Congress affirmatively endorsed the President's actions.[176]

In advancing the first and third arguments, the administration relies upon a broad interpretation of the 2001 joint resolution of Congress referred to as the Authorization for Use of Military Force (AUMF).[177] Congress passed the AUMF in the wake of the September 11 terrorist attacks and in anticipation of an armed invasion of Afghanistan.[178] Congress and the President worked in concert over two hectic days to draft and pass the joint resolution.[179] The resulting resolution passed on September 14, 2001 includes a long preamble detailing the terrorist attacks and the need for a national response followed by a general paragraph that states:

---

[170] FISA, 50 U.S.C. § 1811.

[171] *Id.*

[172] H.R. REP. NO. 95–1720, at 34 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4063.

[173] *See* DOJ WHITE PAPER, *supra* note 24, at 6–13, 17–28.

[174] *Id.* at 17–28 (arguing that the surveillance program satisfied the FISA statutory framework).

[175] *Id.* at 6–10 (discussing the President's inherent power).

[176] *Id.* at 10–13 (discussing Congress's endorsement of the President's actions).

[177] *See id.* at 10–13, 17–28; *see also* Authorization for Use of Military Force (AUMF), Pub. L. No. 107–40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 (2000 & Supp. III 2003)).

[178] *See* RICHARD F. GRIMMETT, AUTHORIZATION FOR USE OF MILITARY FORCE IN RESPONSE TO THE 9/11 ATTACKS (P.L. 107–40): LEGISLATIVE HISTORY 1–2 (CONG. RES. SERV. 2006), *available at* http://www.fas.org/sgp/crs/natsec/RS22357.pdf (providing the legislative history of the passage of the AUMF); Tom Daschle, Editorial, *Power We Didn't Grant*, WASH. POST, Dec. 23, 2005, at A21.

[179] *See* GRIMMETT, *supra* note 178, at 1–2; Daschle, *supra* note 178.

> That the 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.[180]

The administration argues that the broad language of the AUMF, including the phrase "all necessary and appropriate force," implicitly authorized the President to conduct the warrantless surveillance of domestic targets.[181] In addition, the administration relies upon the 2004 United States Supreme Court case, *Hamdi v. Rumsfeld*,[182] that interpreted the AUMF broadly enough to authorize the detention of an American citizen captured on the battlefield of Afghanistan.[183]

The administration errs, however, when interpreting the AUMF to include electronic surveillance of domestic targets because: (1) the legislative history demonstrates the limited authority granted to the President and (2) the *Hamdi* holding does not extend the "battlefield" to which the AUMF applies to the United States.

A. The Legislative History of the AUMF Demonstrates a Limited Grant of Authority

The legislative history of the AUMF is sparse due to its quick enactment resulting from a decision to forego the formal committee legislative review process.[184] A comparison of the White House and congressional drafts of the joint resolution and the public statements made during the drafting process provides some information on the extent of authority granted.[185] The original draft resolution provided by the White House contained broad language that would authorize the President to use force against the perpetrators of the September 11 attacks, as well as "to deter and pre-empt any future acts of terrorism or aggression against the United States."[186] This last provision authorized force without any requisite nexus between the threat of attack and the perpetrators of the September 11 attacks.[187] Richard Grimmett, in his Congressional Research Service Report for Congress on this issue, states that this portion of the draft resolution sparked strong opposition in Congress, when a concern about the extent

---

[180] *See* GRIMMETT, *supra* note 178, at 6 (containing the text of the joint resolution for the Authorization for Use of Military Force, September 14, 2001).

[181] *See* DOJ WHITE PAPER, *supra* note 24, at 10–13.

[182] 542 U.S. 507 (2004).

[183] *Id.* at 519; *see* DOJ WHITE PAPER, *supra* note 24, at 12–13.

[184] *See* GRIMMETT, *supra* note 178, at 2.

[185] *See id.* at 2–3.

[186] *Id.* at 5–6 (providing the text of the original White House proposal).

[187] *See id.*

of the authorization led to a key amendment to the resolution.[188] The joint resolution that resulted limited the grant of authorization to the use of force against those involved in the attacks on September 11.[189] The modification Congress made to the White House draft makes clear that the extent of the authorization does not apply to terrorists generally but only to those people or parties directly connected to the attacks.[190]

Former Senator Daschle, who helped negotiate the joint resolution, also recounted after the revelation of NSA surveillance in December 2005 that the administration sought to add the term "in the United States" after "appropriate force" in the text of the resolution.[191] Senator Daschle explained that this addition "would have given the president broad authority to exercise expansive powers not just overseas—where we all understood he wanted authority to act—but right here in the United States, potentially against American citizens."[192] The administration, by seeking this amendment, clearly demonstrated its understanding that its power was limited to overseas.[193] Thus, based on this legislative history, the AUMF did not authorize the use of electronic surveillance for domestic terminals but restricted the extent of the authority given to the President to prosecute armed conflict overseas.[194]

B. The Hamdi *Holding Does Not Extend the "Battlefield" to Which the AUMF Applies to the United States*

The Attorney General also makes the argument for a broad reading of the AUMF based upon the United States Supreme Court plurality opinion in *Hamdi v. Rumsfeld*.[195] In *Hamdi*, the Court addressed the issue of whether the AUMF constituted an "Act of Congress" that would render the Non-Detention Act inapplicable to the capture of an American citizen.[196] The administration argued for a broad interpretation of the AUMF that would allow the government to bypass the Non-Detention Act and detain American citizens indefinitely based on the authority granted by the AUMF.[197] The

---

[188] *See id.* at 2–3.

[189] The language was changed to authorize necessary force "to prevent any future acts of international terrorism against the United States *by such nations, organizations or persons*." (emphasis added). AUMF, 50 U.S.C. § 1541.

[190] *See* GRIMMETT, *supra* note 178, at 3.

[191] Daschle, *supra* note 178.

[192] *Id.*

[193] *See id.*

[194] *See id.*; *see also* GRIMMETT, *supra* note 178, at 2–3.

[195] 542 U.S. 507 (2004).

[196] *Id.* at 510–11, 516–17. The applicable section of the Non-Detention Act reads: "No citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress." 18 U.S.C. § 4001(a) (2000).

[197] *Hamdi*, 542 U.S. at 517.

Supreme Court agreed with the government's conclusion, but it did so by applying a much narrower interpretation of the AUMF.[198]

Instead of reading the AUMF as a broad authorization of force against terrorism generally, the Court provided a narrow holding that the AUMF authorizes that

> [t]he United States may detain, for the duration of these hostilities, individuals legitimately determined to be Taliban combatants who "engaged in an armed conflict against the United States." If the record establishes that United States troops are still involved in active combat in Afghanistan, those detentions are part of the exercise of "necessary and appropriate force," and therefore are authorized by the AUMF.[199]

When the military detained an American citizen who fell within this category, he or she could be detained for the duration of the active hostilities because detention constituted an important incident of war.[200] The Court went on to find active hostilities to be ongoing by referencing a conventional indication of armed conflict—troop strength—to demonstrate that Afghanistan remained a battlefield and then proceeded to distinguish the Civil War era Supreme Court case of *Ex parte Milligan*.[201] *Milligan* stands for the proposition that American citizens may not be tried by military tribunals when they are not captured on the battlefield of war.[202] In *Milligan*, the incident to war—military tribunals—could only be properly employed in a battlefield where Article III courts were inoperable.[203] The Court in *Hamdi* applied the equivalent of the *Milligan* battlefield concept and narrowly held detention—the incident of war at issue—proper when an American citizen is captured on the battlefield.[204]

The *Hamdi* holding, therefore, does not aid the administration in justifying the NSA surveillance pursuant to the AUMF.[205] In fact, the administration misstates the holding when it says that *Hamdi* "authorize[s] the detention of an American within the United States."[206] The Court in *Hamdi* clearly stated that the narrow issue addressed was whether an American citizen found on the battlefield in Afghanistan

---

[198] *See id.* at 518–20.

[199] *See id.* at 521.

[200] *See id.* at 518–20.

[201] *See id.* at 521–22.

[202] *See Ex parte* Milligan, 71 U.S. (4 Wall.) 2, 127 (1866) ("If, in foreign invasion or civil war, the courts are actually closed, and it is impossible to administer criminal justice according to law, then, on the theatre of active military operations, where war really prevails, there is a necessity to furnish a substitute for the civil authority, thus overthrown, to preserve the safety of the army and society . . . .").

[203] *Id.*

[204] *See Hamdi*, 542 U.S. at 521–22.

[205] *See id.*

[206] *See* DOJ WHITE PAPER, *supra* note 24, at 12.

could be detained in contravention of the Non-Detention Act.[207] The Court's holding does not reach whether an American citizen could have been detained within the United States pursuant to the AUMF, which would provide the pure analogy.[208]

To apply *Hamdi*, one must recognize the incident of war at issue to be electronic surveillance instead of detention but the battlefield would, as in *Hamdi*, be limited to the field of traditional, armed conflict (Afghanistan).[209] The battlefield would not extend to include domestic terminals within the United States, much as the battlefield of the Civil War did not extend into the state of Indiana.[210] If it did, then the natural expansion would be, as Robert Levy at the Cato Institute points out, that the AUMF would apply to pure domestic to domestic terminal surveillance as well.[211] If Indiana did not constitute a battlefield during the Civil War, New Jersey certainly does not constitute a battlefield when the armed forces are engaged in Afghanistan.[212]

This interpretation of the AUMF is consistent with the recent five-three decision of *Hamdan v. Rumsfeld*, in which the Supreme Court addressed the President's power to establish military tribunals for suspected terrorists being held in Guantanamo Bay, Cuba.[213] In interpreting the AUMF, the Court found nothing in the text of legislative history hinting that Congress wanted to alter the provisions of the Uniform Code of Military Justice.[214] Justice Breyer, in his concurrence, characterized it this way: "Congress has not issued the Executive a 'blank check.'"[215]

C. Congress Speaks After the AUMF: Subsequent Amendments to the Foreign Intelligence Surveillance Act

The Bush administration also proceeds with its arguments for the legality of the warrantless electronic surveillance under the supposition that the AUMF represents

---

[207] *Hamdi*, 542 U.S. at 516, 519.

[208] *See id.* at 519.

[209] *See id.* at 521–22.

[210] *See id.*; *Ex parte* Milligan, 71 U.S. (4 Wall.) 2, 127 (1866).

[211] *See Wartime Executive Power and the NSA's Surveillance Authority II: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 7 (2006) (statement by Robert A. Levy, Ph.D., J.D., Senior Fellow in Constitutional Studies, Cato Institute), *available at* http://www.constitutionproject.org/pdf/levy_testimony_02_28_06.pdf [hereinafter *Wartime Executive Power Hearings*] ("The same logic that argues for warrantless surveillance of foreign-to-domestic and domestic-to-foreign communications would *permit warrantless surveillance of all-domestic communications as well*." (emphasis added)).

[212] *See Milligan*, 71 U.S. at 127.

[213] 126 S. Ct. 2749 (2006). It was a five-three decision with Justice Stevens writing for the majority. Justices Kennedy and Breyer joined in the opinion, each writing separate concurrences. The three dissenters were Justices Scalia, Thomas, and Alito. Chief Justice Roberts, who participated in the lower court decision, took no part in the decision.

[214] *See id.* at 2775.

[215] *See id.* at 2799 (Breyer, J., concurring).

the most recent congressional action on the issue of electronic surveillance.[216] Congress has, however, spoken multiple times since September 18, 2001, the date of the enactment of the AUMF, on this issue through statutory amendments to FISA.[217] The most substantial amendments to FISA came from the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act).[218] In addition to the PATRIOT Act, Congress also has made substantial amendments through the Intelligence Authorization Act for Fiscal Year 2002,[219] the Homeland Security Act of 2002,[220] the Intelligence Reform and Terrorism Prevention Act of 2004,[221] and the USA PATRIOT Improvement and Reauthorization Act of 2005.[222]

The amendments to FISA were not passed solely on congressional initiative but were passed, ironically, in response to needs identified by the Bush administration.[223] President Bush, in an address to the nation and to a Joint Session of Congress on September 20, 2001, stated, "We will come together to give law enforcement the additional tools it needs to track down terror here at home. We will come together to strengthen our intelligence capabilities, to know the plans of terrorists before they act and find them before they strike."[224] He also recognized the continued vitality of a court order process when he said,

> When we're talking about chasing down terrorists, we're talking about getting a court order before we do so. It's important for our fellow citizens to understand, when you think PATRIOT Act, constitutional guarantees are in place when it comes to doing what is necessary to protect our homeland, because we value the Constitution.[225]

This and similar statements made by the President identified the need for changes to the existing FISA structure, but they also implied the continued vitality of FISA requirements and the intent to act within those statutory requirements.[226]

---

[216] *See generally* DOJ WHITE PAPER, *supra* note 24.

[217] *See* BAZAN, *supra* note 117, at exsum.

[218] Pub. L. No. 107–56, 115 Stat. 272 (2001) (codified at scattered sections in 50 U.S.C. (2000 & Supp. III 2003)).

[219] Pub. L. No. 107–108, 115 Stat. 1394 (2001).

[220] Pub. L. No. 107–296, 116 Stat. 2135 (2002).

[221] Pub. L. No. 108–458, 118 Stat. 3638 (2004).

[222] Pub. L. No. 109–177, 120 Stat. 192 (2006).

[223] *See* President's Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11 (Sept. 20, 2001), 37 WEEKLY COMP. PRES. DOC. 1347, 1350 (Sept. 24, 2001) [hereinafter Sept. 20, 2001 Address].

[224] *Id.*

[225] Apr. 20, 2004 Remarks, *supra* note 1, at 641.

[226] *See id.*; Sept. 20, 2001 Address, *supra* note 223, at 1350.

Congress responded to the call for changes to FISA by providing the President and the executive branch additional flexibility to conduct electronic surveillance under FISA.[227] The PATRIOT Act made significant modifications to the scope of surveillance allowed under FISA and increased the bureaucratic ability of the FISC to handle more FISA applications.[228] Specifically, the PATRIOT Act provided additional district court judges, roving and multipoint electronic surveillance authority, more flexibility for pen registers and trap and trace devices, and additional access to business records.[229]

The PATRIOT Act also made a significant modification that lessened the requirement for valid electronic surveillance from one with the primary purpose of obtaining foreign intelligence to one with a *significant* purpose.[230] Congress intended that the change promote the sharing of information between the intelligence community and the law enforcement community.[231] In addition, Congress recognized the overlap between traditional law enforcement purposes and intelligence purposes, and it sought to ensure that FISA did not restrict the use of the statutory framework in cases when this overlap existed.[232] The Court of Review, in *In re Sealed Case*, affirmed this interpretation of the addition of the word "significant" and held that it allowed the government to use the FISC order to conduct electronic surveillance as long as some broader objective existed than solely criminal prosecution.[233]

The PATRIOT Act also expanded the authority to address two concerns uniquely associated with the terrorist threat: (1) roving or multipoint surveillance[234] and (2) the "lone wolf" amendment.[235] Through the allowance for roving or multipoint surveillance, Congress sought to modernize FISA to allow the government to continue to intercept a terrorist's communications despite the target changing cell phones frequently or moving from safehouse to safehouse without having to return for a new court order for each new phone or landline used.[236] The "lone wolf" amendment

---

[227] *See* BAZAN, *supra* note 117, at exsum, 1.

[228] *See id.* at 1.

[229] *Id.*

[230] *See id.* at 15–16; Mary De Rosa, Summary of Andrew C. McCarthy & David Cole, *Section 218: Amending the FISA Standard*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT 65–66 (Stewart A. Baker & John Kavanagh eds., 2005) [hereinafter DeRosa, *Section 218*]; McNabb & McNabb, *supra* note 46, at 15.

[231] DeRosa, *Section 218*, *supra* note 230, at 65.

[232] *See id.* at 65–66.

[233] 310 F.3d 717, 735 (FISA. Ct. Rev. 2002).

[234] *See* Mary DeRosa, Summary of James X. Dempsey & Paul Rosenzweig, *Section 206: Roving Surveillance Authority Under FISA*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT 17 (Stewart A. Baker & John Kavanagh eds., 2005) [hereinafter DeRosa, *Section 206*].

[235] *See* Mary DeRosa, Summary of Michael J. Woods & Suzanne Spaulding, *Intercepting Lone Wolf Terrorists*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT 81 (Stewart A. Baker & John Kavanagh eds., 2005) [hereinafter DeRosa, *Intercepting Lone Wolf Terrorists*].

[236] *See* DeRosa, *Section 206*, *supra* note 234, at 17–18.

broadened the FISA definition of an "agent of a foreign power" to include individuals for whom no affiliation with a foreign power or entity could be established.[237] Once again, the intent of the amendment sought to encourage the use of the FISA statutory framework for terrorist suspects.[238]

Finally, the Intelligence Authorization Act for Fiscal Year 2002 made one additional and extremely relevant modification to the emergency exception to the general FISC order process.[239] The amendment authorizes the Attorney General to conduct electronic surveillance in an emergency situation for seventy-two hours.[240] FISA previously provided only twenty-four hours.[241] The result is a practical concession that the executive branch may need the flexibility to conduct such surveillance to address the modern terrorist threat.[242]

Congress's amendments to FISA demonstrate the intent that the FISA framework for electronic surveillance survived despite the joint resolution authorizing the President to commit the armed forces following the September 11 attacks. Even if we were to accept the argument that Congress had spoken through its legislation and the AUMF did control electronic surveillance in contravention to the FISA framework, this authority would have been limited to the time required for Congress to react and speak again on this issue.[243] This interpretation would be consistent with the congressional intent associated with the declaration of war exception to the general court order process, which was intended to provide the President a short period of executive discretion, followed by congressional adaptation to the situation by statute.[244]

IV. FAILURE TO FOLLOW FISA AND ITS CONSTITUTIONAL RAMIFICATIONS

A. The Failure to Satisfy the FISA Framework

Attorney General Alberto Gonzalez, in his Department of Justice White Paper supporting the legality of the NSA surveillance, argues that the electronic surveillance conducted conforms and is "fully consistent with the requirements of the Foreign Intelligence Surveillance Act . . ."[245] The Attorney General does not define "fully con-

---

[237] *See* DeRosa, *Intercepting Lone Wolf Terrorists*, *supra* note 235, at 81.

[238] *See id.*

[239] *See* BAZAN, *supra* note 117, at 23 & n.40. For a detailed explanation of the emergency exception, see *supra* notes 163–69 and accompanying text.

[240] *See* BAZAN, *supra* note 117, at 23 & n.40.

[241] *Id.* at 23 n.40.

[242] *See id.* at 23 & n.40.

[243] *See* H.R. REP. NO. 95–1720, at 34 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4063; DOJ WHITE PAPER, *supra* note 24, at 20. This time period would have ended with the passage of the USA Act on October 12, 2001. The USA Act was the precursor to what eventually became the USA PATRIOT Act, which passed on October 26, 2001. Pub. L. 107–56, 115 Stat. 272 (2001).

[244] *See* H.R. REP. NO. 95–1720, at 34, 1978 U.S.C.C.A.N. at 4063.

[245] DOJ WHITE PAPER, *supra* note 24, at 17.

sistent," however, to mean full compliance.[246] Instead, the Bush administration's argument is that FISA envisions scenarios where the statutory requirements would be inapplicable to the President.[247] Specifically, the administration relies upon section 1809, which details the criminal sanctions levied upon one who conducts prohibited surveillance, and its provision that "[a] person is guilty of an offense if he intentionally . . . engages in electronic surveillance under color of law *except as authorized by statute*." (the Exception Clause).[248] This argument then relies upon the Authorization for Use of Military Force (AUMF)—the Congressional Joint Resolution passed in the wake of the September 11 terrorist attacks—as the authorizing statute.[249]

It is important to note that this far-fetched argument surfaced as the President scrambled to justify the warrantless NSA surveillance.[250] In fact, during a press conference on December 19, 2005, three days after the public learned about the warrantless surveillance, the President justified the surveillance by distinguishing FISA as a framework for long-term monitoring, as opposed to the need for warrantless surveillance to "detect" terrorists.[251] The President's statements show an awareness, or at least a belief, that the nature of the NSA surveillance operated outside of the mandates of FISA but did not rest on a belief that the operations satisfied the FISA requirements, even to the technical extent argued by Attorney General Gonzalez.[252]

Even assuming that the President understood and justified the surveillance based upon this technical and myopic view of the FISA provision, the argument lacks merit due to the statutory interpretation of the "authorized by statute" provision, especially in light of its legislative purpose.[253] In addition, the AUMF provides a use of force resolution that the FISA framework specifically contemplated, making this argument disingenuous and calling into question the President's constitutional requirement that he "take Care that the Laws be faithfully executed."[254]

---

[246] *See id.* at 17–23.

[247] *See id.* at 20–21. In fact, this argument is even broader in its application by exempting not only the President from the FISA requirements but any person who conducts the otherwise proscribed activities. *See* FISA, 50 U.S.C. § 1809(a)(1) (2004).

[248] FISA, 50 U.S.C. § 1809(a)(1) (2004) (emphasis added); *see also* DOJ WHITE PAPER, *supra* note 24, at 20.

[249] *See* DOJ WHITE PAPER, *supra* note 24, at 23–28.

[250] The President made no mention of this argument during his press conference on December 19, 2005. *See* Dec. 19, 2005 Press Conference, *supra* note 3.

[251] *See id.* at 1887. The President stated, "there is a difference between detecting, so we can prevent, and monitoring. And it's important to know the distinction between the two." *Id.* at 1889.

[252] *See id.* at 1887; DOJ WHITE PAPER, *supra* note 24, at 20–23.

[253] *See* H.R. REP. NO. 95–1720, at 33 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4062 (adopting the nonconforming House version only for the purpose of providing a good faith defense). This purpose is strengthened by the inclusion of three explicit exceptions to the court order process. *See supra* notes 147–72 and accompanying text.

[254] U.S. CONST. art. II, § 3. For a detailed description of the AUMF, see *supra* notes 173–215 and accompanying text.

FISA specifically expresses and defines the exceptions to its preferred court order process.[255] The Bush administration's reliance on the "except as authorized by statute" provision in the criminal sanctions section of FISA unduly reads an additional exception into this framework.[256] The administration reads this provision broadly to say that it stands for an expansive proposition that any congressional statute that purports to allow for electronic surveillance could authorize presidential action outside the FISA requirements.[257] The administration supports this position and interpretation by comparing the language of the FISA criminal sanctions provision to the Title III criminal sanctions provision.[258] The Attorney General argues that the Title III provision, which states, "[e]xcept as otherwise *specifically provided in this chapter*," shows the ability of Congress to reference internally, and therefore, the different language in FISA shows the intent that it apply more generally and not be limited only to subsequent amendments to FISA or to provisions provided for in Title III.[259] This argument proceeds upon a misunderstanding of both the Title III provision, as well as the language and intent of the provision in FISA.

The legislative history does not conclusively resolve the issue of whether a narrow interpretation of the FISA provision limiting the term "statute" to only FISA and Title III provisions or a broad interpretation that views "statute" as referring to any congressional statute is correct.[260] The House Conference Committee did consider a Senate and House version of what would become section 1809.[261] The Senate bill sought to conform the FISA criminal sanctions provision to Title III and provide that culpability would follow a knowing violation of FISA, "except as provided in this bill."[262] Due to its addition as a conforming amendment to Title III, the Exception Clause would apply only to FISA and Title III provisions.[263] The House version provided for separate criminal penalties from Title III and included the more ambiguous language later adopted.[264] In adopting the House version, the Conference Committee stressed that the choice turned on the desire to include "[a] defense . . . for a defendant who was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to

---

[255] *See* FISA, 50 U.S.C. §§ 1802, 1805(f), 1811 (2004). For a detailed description of these exceptions, see *supra* notes 147–72 and accompanying text.

[256] *See* FISA, 50 U.S.C. § 1809(a)(1); DOJ WHITE PAPER, *supra* note 24, at 20–23.

[257] *See* DOJ WHITE PAPER, *supra* note 24, at 20.

[258] *See id.*

[259] FISA, 18 U.S.C. § 2511(1) (Supp. 2006) (emphasis added); *see* DOJ WHITE PAPER, *supra* note 24, at 20–21.

[260] *See* H.R. REP. NO. 95–1720, at 33 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4062.

[261] *See id.*

[262] *See id.*

[263] *See id.*

[264] *See id.*

a search warrant or court order of a court of competent jurisdiction."[265] The language of this defense closely follows what would be later held by the Supreme Court, in *United States v. Leon*, to constitute a "good faith" exception to the exclusionary rule.[266]

The decisions by the Conference Committee to allow for the equivalent of a "good faith" defense does not counsel either a broad or narrow interpretation of the Exception Clause.[267] It does, however, suggest that Congress did not voice disagreement with the Senate bill's Exception Clause that provided a clear and narrow application to only FISA and Title III provisions, but it focused primarily on including the House's "good faith" defense.[268]

The preference for a narrow interpretation is bolstered, if not confirmed, by the exclusivity provision found in section 2511(2)(f) of Title III.[269] The exclusivity provision states, "[P]rocedures in this chapter or chapter 121 . . . and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted."[270] The House Conference Committee for FISA debated between this language as contained in the Senate bill and a House amendment that would have added the word "statutory" after "exclusive" to modify and restrict the exclusivity.[271] The Conference Committee rejected the House amendment in an attempt to exercise complete congressional power in this area and to apply the standard set forth in Justice Jackson's concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*.[272] Based on this specific legislative history, it is undeniable that Congress, through its language and its intent, sought the provisions of Title III and FISA to provide express and complete congressional authorization in the area of electronic surveillance.[273]

The expressly exclusive nature of Title III and FISA resolves any ambiguity as to the proper interpretation of the Exception Clause in favor of a narrow interpretation that reads "statute" as internally referencing the provisions of FISA and Title III. This interpretation also coincides with the well-settled canon of statutory interpretation

---

[265] *Id.*

[266] 468 U.S. 897, 922 (1984). For further analysis of the development of the "good faith" exception, see Gerald G. Ashdown, *Good Faith, The Exclusionary Remedy, and Rule-Oriented Adjudication in the Criminal Process*, 24 WM. & MARY L. REV. 335, 383–84 (1983). Justice White argued for this exception as early as 1976 in his dissenting opinion in *Stone v. Powell*, in which he argued, in language similar to the FISA statute, that the exclusionary rule should not apply when the evidence "was seized by an officer acting in the good-faith belief that his conduct comported with existing law." 428 U.S. 465, 538 (1976) (White, J., dissenting).

[267] *See* H.R. REP. NO. 95–1720, at 33, 1978 U.S.C.C.A.N. at 4062.

[268] *See id.*

[269] Title III, 18 U.S.C. § 2511(2)(f) (Supp. 2006).

[270] *Id.* (internal citations omitted).

[271] *See* H.R. REP. NO. 95–1720, at 35, 1978 U.S.C.C.A.N. at 4064.

[272] *See id.*; 343 U.S. 579, 637 (1952).

[273] *See* Title III, 18 U.S.C § 2511(2)(f); H.R. REP. NO. 95–1720, at 35, 1978 U.S.C.C.A.N. at 4064.

known as *lex specialis derogat legi generali*, which provides that narrow and specific statutory provisions should supplant general provisions.[274]

B. The AUMF Does Not Supersede the FISA Framework

The administration's theory that the Exception Clause provides legal authority under FISA also fails because the AUMF does not constitute an authorizing statute.[275] The administration argues that the broad language in the joint resolution that authorizes the President "to use all necessary and appropriate force against those nations, organizations, or persons" that aided in the terrorist attacks of September 11 confers upon the President the power to conduct domestic electronic surveillance.[276] As discussed above, the administration incorrectly interprets the AUMF as granting broader authority than either Congress intended or the Supreme Court has recognized.[277] There is no doubt that Congress provided the President the authority to employ the armed forces of the United States against the Taliban in Afghanistan in the effort to catch the members of Al Qaida who were responsible for planning and executing the terrorist attacks. It is a very different contention, however, that this broad and general language specifically authorized the President to circumvent FISA's statutory requirements.[278]

The strongest argument against the administration's position is found in the statutory language of FISA itself.[279] FISA provides an express exception for authorization during a time of war.[280] The President may authorize electronic surveillance without a court order for fifteen days following a declaration of war.[281] The House Conference Committee explicitly addressed this provision and settled on fifteen days to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency."[282] The statutory language and legislative history provide a clear indication that Congress considered the legal framework applicable during wartime and provided a vehicle for a subsequent Congress to provide the President the authority needed to address the immediacy of the situation while Congress reconsidered the statutory guidelines.[283] When this specific language conflicts with a general statutory provi-

---

[274] *See Wartime Executive Power Hearings*, *supra* note 211, at 6; *see also infra* notes 347–64 and accompanying text.

[275] *See Wartime Executive Power Hearings*, *supra* note 211, at 6.

[276] AUMF, 50 U.S.C. § 1541 (2004).

[277] *See supra* notes 173–215 and accompanying text.

[278] *See* DOJ WHITE PAPER, *supra* note 24, at 24; *see also* discussion of Hamdan v. Rumsfeld, *supra* notes 213–14 and accompanying text.

[279] *See* FISA, 50 U.S.C. § 1811 (2004).

[280] *See id.* For a description of the statutory framework of the Authorization During Time of War exception, see *supra* notes 170–72 and accompanying text.

[281] FISA, 50 U.S.C. § 1811. The House amendments to the Senate bill originally called for a one-year time period. H.R. REP. NO. 95–1720, at 34 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4063.

[282] H.R. REP. NO. 95–1720, at 34, 1978 U.S.C.C.A.N. at 4063.

[283] *See id.*; FISA, 50 U.S.C. § 1811.

sion such as the AUMF, the same canon of statutory interpretation described above—*lex specialis derogat legi generali*—counsels application of the specific provision.[284]

In addition, the subsequent amendments to FISA described above demonstrate that the AUMF is not controlling law on the matter of domestic electronic surveillance.[285] The administration assumes throughout its white paper that Congress has not superseded the AUMF but focuses on the ability of the AUMF to provide authority outside of the FISA context.[286] Even if the AUMF did initially exempt the President from the statutory requirements of FISA, the subsequent amendments to FISA present more recent congressional legislation on the issue of electronic surveillance and should control in any analysis under the Exception Clause. There is no contention, even by the Bush administration, that the warrantless electronic surveillance program satisfies the explicit requirements of FISA, even as amended.[287]

C. The President Has No Inherent Constitutional Power to Authorize Warrantless Surveillance

The Bush administration argues that even if the warrantless surveillance program fails to satisfy the requirements of FISA, such surveillance is permissible as an exercise of inherent constitutional power.[288] This argument rests on a belief that the President holds the exclusive power to conduct the electronic surveillance at issue, thus making Congress's efforts to regulate in this area unconstitutional.[289] This assertion, however, is unsound because the President must rely upon concurrent war powers to conduct electronic surveillance, and this would require the President to obtain either congressional authority for the acts or to demonstrate that Congress had not acted within this sphere of authority.[290]

The Constitution distributes power either exclusively or concurrently among the three branches of government.[291] The Framers of the Constitution debated extensively over whether to follow the British model and vest war powers solely in the executive branch or to jettison popular wisdom and distribute them between the executive and

---

[284] *See Wartime Executive Power Hearings*, *supra* note 211, at 6.

[285] *See supra* notes 216–44 and accompanying text.

[286] *See* DOJ WHITE PAPER, *supra* note 24, at 23–28.

[287] *See generally* DOJ WHITE PAPER, *supra* note 24; Dec. 19, 2005 Press Conference, *supra* note 3, at 1889.

[288] *See* DOJ WHITE PAPER, *supra* note 24, at 6–10.

[289] *See infra* notes 305–28 and accompanying text.

[290] *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 634–38 (1952) (Jackson, J., concurring) (describing the three categories of presidential power); LOUIS FISHER, PRESIDENTIAL WAR POWER 1–3, 8–9, 12–16, 20–22 (2d ed. 2004) (describing the legislative history and extent of the President's war power and foreign power authority).

[291] The power of appointment and removal of executive officers is an example of an exclusive power vested solely in the President. The Congress has no power to legislate in this area. Myers v. United States, 272 U.S. 52, 163–64 (1926).

legislative branches.[292] The Framers decided on the latter and vested war powers in Congress through seven clauses in the Constitution, while also providing the President the significant power to direct and control war as the Commander-in-Chief.[293] Due to these constitutional grants, the nation's war powers must be understood to be held concurrently between the executive and Congress. The question that remains is to what extent.

Louis Fisher, in his book *Presidential War Power*, argues that the debates during the Constitutional Convention demonstrate the clear intent by the Framers to hinder the President's ability to employ the military unilaterally.[294] The power to "declare war" granted to Congress provided the legislative body with the ultimate authority to commit the United States armed services to war, while reserving to the President the authority to repel a sudden attack.[295] The notes of the Constitutional Convention maintained by James Madison support this opinion.[296] Roger Sherman, during the debate over whether to define the congressional power as "to make war" or "to declare war" stated, "The Executive sh[ould] be able to repel and not to commence war."[297] Eldridge Gerry and James Madison agreed and chose the word "declare" in an effort to partition war powers along this line—providing the President the ability to repel sudden attacks but vesting Congress with the ultimate authority to bind the nation in war.[298]

---

[292] *See* FISHER, *supra* note 290, at 1–3.

[293] U.S. CONST. art. II, § 2, cl.1. The Constitution gives the Congress power

> To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations;
> To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water;
> To raise and support Armies . . . ;
> To provide and maintain a Navy;
> To make Rules for the Government and Regulation of the land and naval Forces;
> To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions;
> To provide for organizing, arming, and disciplining, the Militia.

U.S. CONST. art. I, § 8, cl.10–16.

[294] FISHER, *supra* note 290, at 8.

[295] *See id.* at 8–9.

[296] JAMES MADISON, NOTES OF DEBATES IN THE FEDERAL CONVENTION OF 1787, at 475–77 (Ohio Univ. Press 1966).

[297] *Id. at* 476. Roger Sherman was the only person to have signed all four major founding documents: the Continental Association of 1774, the Declaration of Independence, the Articles of Confederation, and the United States Constitution. USHistory.org, Signers of the Declaration of Independence: Roger Sherman, http://www.ushistory.org/declaration/signers/sherman.htm (last visited Aug. 23, 2006).

[298] *See* MADISON, *supra* note 296, at 476. Central to the delineation of war powers was the idea that the making of peace, which required Presidential action and Senate approval, should be more flexible than the facilitation of war. *Id.* The decision to vest greater power in Congress to make and prosecute a war was, in fact, a conscious decision and an effort to hinder the ability

The concurrent nature of war powers is evidenced by their employment throughout American history.[299] Congress has passed eleven separate formal declarations of war and numerous authorizations for the use of force, and in most cases Congress granted the authority after a President's request.[300] Presidents in the post-World War II era, however, have argued and acted against this concurrent power.[301] Military actions in Grenada, Panama, Somalia, and Kosovo, in addition to President Truman's use of force in Korea, all began and were conducted without congressional authorization.[302] Congress fought the erosion of its concurrent power by passing the War Powers Resolution (WPR) in 1973 in an attempt to statutorily limit the President's use of force.[303] In fact, the WPR seeks to reassert Congress's concurrent war powers, despite actually ceding some constitutional powers to the President.[304] The fact that multiple presidents have taken dubious constitutional positions on the use of force does not justify or validate such actions or change the limits of constitutional language and intent. In fact, when viewing the list of military actions taken without congressional approval, the wisdom of the Framers appears reinforced.

The Bush administration rejects that concurrent power exists to conduct warrantless foreign intelligence surveillance.[305] The administration does not contend, however, that this inherent authority derives solely from the President's war powers as Commander-in-Chief.[306] Instead, the administration relies on the theory that the President is the "sole organ" of foreign affairs.[307] The "sole organ" theory is implied from the President's role as the prime communicator between the United States and other nations, and supporters often cite to John Marshall's statement on March 7, 1800, in the House of Representatives, that "[t]he President is the sole organ of the

---

of the nation to continue a war unless the President enjoyed the nation's support. *See id.*

[299] *See generally* DAVID M. ACKERMAN & RICHARD F. GRIMMETT, DECLARATIONS OF WAR AND AUTHORIZATIONS FOR THE USE OF MILITARY FORCE: HISTORICAL BACKGROUND AND LEGAL IMPLICATIONS exsum (CONG. RES. SERV. 2003), *available at* http://www.fas.org/sgp/crs/natsec/RL31133.pdf (providing a historical background on declarations of war and authorizations for the use of military force).

[300] *Id.* The eleven separate formal declarations of war were in the context of five wars and were against: (1) Great Britain (1812), (2) Mexico (1846), (3) Spain (1898), (4) Germany (1917), (5) Austria-Hungary (1917), (6) Japan (1941), (7) Germany (1941), (8) Italy (1941), (9) Bulgaria (1942), (10) Hungary (1942), and (11) Rumania (1942). *Id.* at 4–6. For a list and brief description of major examples of congressional authorization of military force, *see id.* at 6–20.

[301] *See* JOHN YOO, THE POWERS OF WAR AND PEACE: THE CONSTITUTION AND FOREIGN AFFAIRS AFTER 9/11, at 12 (2005).

[302] *Id.*

[303] *See id.*; FISHER, *supra* note 290, at 144–45.

[304] *See* FISHER, *supra* note 290, at 144–45.

[305] DOJ WHITE PAPER, *supra* note 24, at 6.

[306] *See id.* at 6–7.

[307] *See id.* at 6–7 (citing United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936)).

nation in its external relations, and its sole representative with foreign nations."[308] This authority over foreign affairs may intersect with war powers because supporters of the sole organ theory argue that the President, acting under this authority, "may initiate military operations to fulfill the foreign policy."[309] The Bush administration espouses this idea by citing to the Supreme Court case of *United States v. Curtiss-Wright Export Corp.*, which held what Marshall argued—that the President has plenary power in the field of international relations.[310] The administration then applies this foreign affairs power and presumes its foundation for the assertion that the President's power "to protect the Nation from foreign attack" includes the ability to conduct electronic surveillance to achieve that aim.[311]

The administration's argument that the President's foreign affairs power provides inherent authority to conduct warrantless electronic surveillance fails for two reasons: (1) the administration improperly defines the collection of foreign intelligence to include domestic terminal surveillance and (2) the presidential power to protect the nation from attack does not originate in the power over foreign affairs.

First, the argument that the President has the inherent power to conduct warrantless electronic surveillance to collect purely "foreign intelligence"—foreign terminal to foreign terminal communication—is correct and undisputed.[312] The legislative history of FISA does not recognize explicitly that the collection of wholly overseas communication is an inherent presidential power, but it also does not seek to reach and regulate that area of collection.[313] The Church Committee Hearings also sought to differentiate among foreign terminal to foreign terminal communications and those that include either the targeting of a U.S. person or a domestic terminal.[314] The policy behind placing this authority in the hands of the President is that the effects of overreaching would damage diplomatic relations and not the civil liberties of a U.S. person.[315] Diplomatic issues are better left to the President under his foreign affairs power and responsibilities.[316]

The Bush administration unduly expands the term foreign intelligence to include foreign terminal to domestic terminal communications.[317] The inclusion of domestic places and persons in the surveillance authorized exceeds the scope of the President's

---

[308] 10 ANNALS OF CONG. 613 (1800), *available at* http://memory.loc.gov/ammem/amlaw/lwaclink.html#anchor6.

[309] FISHER, *supra* note 290, at 21.

[310] 299 U.S. 304, 319–20 (1936); DOJ WHITE PAPER, *supra* note 24, at 6–7.

[311] *See* DOJ WHITE PAPER, *supra* note 24, at 7.

[312] *See Wartime Executive Power Hearings*, *supra* note 211, at 10 (statement by Robert A. Levy).

[313] S. REP. NO. 95–701, at 34–35 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 4003–04.

[314] *See Church Hearings*, *supra* note 7, at 138–39 (statements between Sen. Frank Church and Philip B. Heymann, Professor of Law, Harvard Law School).

[315] *See Curtiss-Wright Exp. Corp.*, 299 U.S. at 319–20.

[316] *See id.*

[317] *See* DOJ WHITE PAPER, *supra* note 24, at 6–7; Risen & Lichtblau, *supra* note 6.

foreign affairs power.[318] The reliance on the widely criticized *Curtiss-Wright* case to support this proposition also proves the deficiency of the argument.[319] In *Curtiss-Wright*, the Court provided an expansive holding on presidential power in the realm of international relations by addressing the ability to impose arms embargoes in South America.[320] The Court explained its holding, however, by distinguishing between domestic and foreign power, limiting its holding to expansive authority for foreign power.[321] The holding of *Curtiss-Wright*, therefore, does not extend to support presidential actions against domestic persons and places.[322] To act within the domestic sphere on this issue, the President would need to exercise his war powers—powers shared concurrently with Congress—and not rely solely on his broader foreign affairs power.

Second, the Bush administration reaches the erroneous conclusion that the foreign relations power justifies warrantless domestic surveillance by appealing to the President's authority and duty to prevent and repel a sudden attack.[323] It is widely accepted that a President is empowered with this authority.[324] What prompts disagreement is the Bush administration's claim that this power comes from the more expansive foreign affairs powers and not the decidedly concurrent war powers shared with Congress.[325] The history of the Constitutional Convention demonstrates that the Framers thought this power to be part of the general delegation of war powers held concurrently between Congress and the President.[326] It was conceded by opponents that the President must have power in an emergency to act independently of Congress, especially given the concerns expressed during the Convention debates that a Congress meeting only once per year could not react quickly enough to counter immediate threats.[327]

This power contemplated unilateral presidential action, but that power would fall within a limited scope of emergency authorization and then could be limited by con-

---

[318] *See Curtiss-Wright Exp. Corp.*, 299 U.S. at 320. For a discussion of the deficiencies of *Curtiss-Wright* and of the modern acceptance of the President as the "sole organ" of foreign affairs, see Saikrishna B. Prakash & Michael D. Ramsey, *The Executive Power over Foreign Affairs*, 111 YALE L.J. 231 (2001).

[319] *See* FISHER, *supra* note 290, at 69–73.

[320] *See Curtiss-Wright Exp. Corp.*, 299 U.S. at 311–12, 319; *see also* FISHER, *supra* note 290, at 69.

[321] *See Curtiss-Wright Exp. Corp.*, 299 U.S. at 319, 321; *see also* FISHER, *supra* note 290, at 69.

[322] The *Curtiss-Wright* case also involves congressional endorsement on the issue faced by the Court. Though this case was decided before the framework of presidential power provided by Justice Jackson's concurrence in *Youngstown*, the issuance by Congress of a joint resolution supporting the exercise of presidential power would have placed the President's action at the apex of power. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 634–38 (1952) (Jackson, J., concurring); *Curtiss-Wright Exp. Corp.*, 299 U.S. at 311–12.

[323] DOJ WHITE PAPER, *supra* note 24, at 7.

[324] *See* FISHER, *supra* note 290, at 8–9.

[325] *See id.*

[326] *Id.*

[327] MADISON, *supra* note 296, at 475 (statement by Charles Pinkney).

gressional action once the legislative body had the time to assemble and speak under its war powers on the issue.[328] President Bush's reliance on the power to repel a sudden attack, therefore, relies upon war powers shared concurrently with Congress.

D. The President's Authority for Electronic Surveillance Falls into the Third Youngstown *Category*

The modern approach to the constitutional validity of a presidential action derives from Justice Jackson's concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*.[329] *Youngstown* challenged President Truman's seizure of steel mills amidst a nationwide strike of steelworkers.[330] President Truman invoked his powers as Commander-in-Chief to justify the seizure because of the indispensable nature of steel production to the war effort in Korea.[331] Justice Jackson recognized that presidential power is not always fixed, but that it may fluctuate in strength due to the relationship between the President and Congress on the contested issue.[332]

The Court held President Truman's seizure order unconstitutional.[333] In doing so, Justice Jackson, in a concurrence, provided the framework now relied upon to adjudge presidential power.[334] Jackson sought not to delimit a President's power to act in an emergency but to provide three analytical categories that allow for a fluctuation of power dependent upon congressional support.[335] The categories Jackson provided are: (1) the presidential power is at its apex when the President acts pursuant to an express or implied authorization of Congress, (2) the presidential power is within a "zone of twilight" when the President acts in absence of either a congressional grant or denial of authority, and finally (3) the presidential power is at the "lowest ebb" of power when measures are taken that are incompatible with the expressed or implied will of Congress.[336]

Although the *Youngstown* categories are logical and largely outcome determinative once a presidential action is assigned, the difficult part is determining whether the action contravenes congressional action.[337] In *Youngstown*, Justice Jackson concluded that the steel seizure order conflicted with congressional legislation upon the

---

[328] *See id*. at 475–76. This same theory prompted the drafters of FISA to provide for a fifteen day emergency action clause in the event of a declaration of war. This would give the President the ability to conduct electronic surveillance to repulse a sudden attack, while limiting this authority to the time required for Congress to meet, deliberate, and legislate in response to the emergency. *See* H.R. REP. NO. 95–1720, at 34 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4063.

[329] 343 U.S. 579, 634–38 (1952) (Jackson, J., concurring).

[330] *Id*. at 582–83 (majority opinion).

[331] *Id*. at 641–42 (Jackson, J., concurring).

[332] *Id*. at 635.

[333] *Id*. at 588–89 (majority opinon).

[334] *Id*. at 634–38 (Jackson, J., concurring).

[335] *Id*. at 635–38.

[336] *Id*. at 635–37.

[337] *See id*.

"occasions, grounds and methods for seizure of industrial properties."[338] Jackson found that Congress occupied the field of industry seizures through the Selective Service Act of 1948, the Defense Production Act of 1950, and the Labor Management Relations Act, 1947.[339] After finding the field occupied, Jackson concluded that the third category of constitutional power applied to invalidate the seizure order.[340] Once the third category applied, the presidential action could only survive constitutional scrutiny if the President held the power exercised exclusive of Congress.[341]

The application of the *Youngstown* principles to the warrantless NSA surveillance depends primarily on the characterization of the congressional action on this issue. The Bush administration argues that the congressional joint resolution in 2001 for the AUMF endorsed the presidential action and placed the power exercised in the first *Youngstown* category.[342] The counter-argument is that FISA occupies the field of such electronic surveillance and its provisions were not supplanted by the passage of the AUMF.[343]

The AUMF contains broad statements of purpose and general provisions capable of many interpretations regarding the scope of power authorized.[344] If no congressional voice had sounded in the area of electronic surveillance, the argument for implied authorization by Congress through the AUMF may have been stronger. This is, however, not the case.

Congress provided clear statements during the passage of FISA to demonstrate intent to provide the exclusive and exhaustive procedure for the use of electronic surveillance to collect foreign intelligence.[345] In the summary of the FISA legislation passed by the House of Representatives, this intent was clearly expressed by the statement: "The bill . . . combined with chapter 119 of title 18 [Title III] . . . constitutes the exclusive means by which electronic surveillance, as defined, and the interception of domestic wire and oral communications may be conducted; the bill recognizes no inherent power of the President in this area."[346]

---

[338] *Id.* at 639.

[339] *Id.* at 639 n.6–8.

[340] *Id.* at 640.

[341] *Id.*

[342] DOJ WHITE PAPER, *supra* note 24, at 11.

[343] *See Wartime Executive Power Hearings*, *supra* note 211, at 6–8.

[344] *See, e.g.*, AUMF, 50 U.S.C. § 1541 (2000 & Supp. II 2004) ("That the President is authorized to use all necessary and appropriate force . . . .").

[345] *See* S. REP. NO. 95–604, pt. 1, at 5–6 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3907. The legislation so completely occupied the field of electronic surveillance that it actually prompted Senator James Abourezk to oppose the measure because of its exclusive nature. In his minority views, Senator Abourezk argued that the President should have some power in this area, but that the legislation foreclosed the ability of the President to exercise any power in this area outside of the statutory framework. *See id.* at 82, 1978 U.S.C.C.A.N. at 3967.

[346] *Id.* at 6, 1978 U.S.C.C.A.N. at 3907.

Prior to the passage of FISA, the only statutory restrictions on electronic surveillance existed for purely domestic criminal action through Title III.[347] Title III included a disclaimer clause found in the original section 2511(3) that did not disturb presidential power in this area.[348] When Congress enacted FISA, it amended that provision in Title III to remove any deference to presidential prerogative in the area of electronic surveillance.[349]

In addition to the clear congressional intent to occupy the field of electronic surveillance, Congress also anticipated a *Youngstown* inquiry into this issue.[350] The House Conference Committee stated that "[t]he intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case," and to place presidential power in the area of electronic surveillance at its "lowest ebb."[351]

No justification exists for the position that the general authorization language of the AUMF supersedes the specific and exclusive language of FISA.[352] FISA specifically contemplates the applicability of its statutory framework despite the declaration of war.[353] In order for the AUMF to authorize the warrantless NSA surveillance, authority by implication from a general statute would have to govern over the specific regulation found in FISA.[354] Such a result would be inconsistent with both case law and generally accepted rules of statutory construction.

When two statutory provisions conflict, the canon of statutory interpretation *lex specialis derogat legi generali* provides that narrow and specific statutory provisions should supplant general provisions.[355] The Court recognized this principle of statutory interpretation that the specific governs the general in *Morales v. Trans World Airlines, Inc.*, in which the Supreme Court rejected the assertion that a general statutory clause governing available remedies governs over a specific substantive preemption provision.[356] The Supreme Court also settled a question of conflicting statutes by holding that a specific statute governs the general in *International Paper*

---

[347] Title III, Pub. L. 90–351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (1976)).

[348] Title III, 18 U.S.C. § 2511(3) ("Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.").

[349] *See* H.R. REP. NO. 95–1720, at 35 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4064.

[350] *Id.*

[351] *Id.*

[352] *See, e.g.*, Cole et al., *supra* note 115.

[353] *See* FISA, 50 U.S.C. § 1811.

[354] *See id.*; AUMF, 50 U.S.C. § 1541 (2000 & Supp. 2002).

[355] *See Wartime Executive Power Hearings*, *supra* note 211, at 6.

[356] 504 U.S. 374, 384–85 (1992) (citing Crawford Fitting Co. v. J. T. Gibbons, Inc., 482 U.S. 437, 445 (1987)); *see also* Cole et al., *supra* note 115, at 42.

Co. v. Ouellette.[357] The Court resolved the question of whether a general provision in the Clean Water Act that preserved an injured party's ability to seek relief superseded the statute's comprehensive regulation and specific provision of remedies.[358] The Court held the specific provisions govern and stated, "we do not believe Congress intended to undermine this carefully drawn statute through a general savings clause . . . ."[359]

Under this principle of statutory interpretation, FISA would govern electronic surveillance unless an authorization of military force provided some unique justification to part with the well-settled principle.[360] This argument, however, was rejected in *Youngstown* in a similar context.[361] The Supreme Court in *Youngstown* rejected the Truman administration's argument that the President's war powers could trump specific congressional statutes that governed the seizure of industrial property.[362] Though Congress never passed an authorization of force in the context of the Korean War, Truman purported to act within the scope of the United Nations Participation Act and in accordance with implied congressional authorization.[363] The Court rejected the argument that a war context could empower the President to dismiss specific congressional regulation on the utilization of a war power.[364]

The Bush administration argues that the AUMF requires a broad reading to supersede FISA.[365] As discussed above, the administration unduly interprets the AUMF to grant more authority than Congress intended to provide or that the Supreme Court has recognized.[366] In addition, an interpretation of the AUMF that authorized domestic surveillance would render the fifteen day exception for a declaration of war provided for in FISA section 1811 meaningless.[367] Upon declaration of war, the fifteen day exception provides a standby statutory authority designed to authorize automatically limited presidential action outside of the scope of the FISA framework.[368] Congress has legislated standby statutory powers both in the formal declaration of war context and in the expanded use of national emergency declarations as a vehicle to allow flexibility in presidential reaction, while retaining congressional statutory control.[369]

---

[357] *See* 479 U.S. 481, 492–94 (1987).

[358] *Id.*

[359] *Id.* at 494.

[360] *See* DOJ WHITE PAPER, *supra* note 24, at 11.

[361] *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 588–89 (1952).

[362] *See id.*

[363] FISHER, *supra* note 290, at 97–98.

[364] *See Youngstown Sheet & Tube Co.*, 343 U.S. at 644–45 (Jackson, J., concurring).

[365] *See* DOJ WHITE PAPER, *supra* note 24, at 12 (explaining the Bush administration's argument).

[366] *See supra* notes 173–215 and accompanying text.

[367] *See* FISA 50 U.S.C. § 1811 (2000 & Supp. 2002).

[368] ACKERMAN & GRIMMETT, *supra* note 299, at 27, 34.

[369] *See* HAROLD C. RELYEA, TERRORIST ATTACKS AND NATIONAL EMERGENCIES ACT DECLARATIONS 1–4 (CONG. RES. SERV. 2005), *available at* http://www.law.umaryland.edu/

The scope of modern standby powers is largely the result of a Senate special committee initially charted in June 1972 to address congressional displeasure with the President's use of war powers in the context of Vietnam.[370] This Senate committee was co-chaired by Senator Frank Church—the same Senator who chaired the Senate hearings that led to the passage of FISA.[371] The committee found that no process existed to terminate automatically national emergency proclamations and sought to modify standby powers to include a limitation in scope and duration.[372] The passage of FISA occurred after the conclusion of these hearings in May 1976 and the hearings' conclusions likely influenced the inclusion of a limited standby authorization in section 1811 in case of a declaration of war.[373]

An authorization of force provides less, or at least no greater, power to the President than a declaration of war.[374] Thus, because Congress demonstrated in FISA the desire to provide standby authorization, it would do damage both to the integrity of the statutory language itself and the obvious contemplation of its application in a time of war to construe a general authorization of force as superseding its provision and leaving it without meaning.

Finally, any ambiguity that remains as to whether Congress intended the AUMF to supersede FISA dissolves when considered in the context of subsequent amendments to FISA.[375] As discussed above, Congress took great strides since September 11 to modify and amend FISA to apply to the current threats of terrorism, while retaining its basic purpose of judicial review.[376] The conclusion that must be drawn from the amendments to FISA is that Congress intended the framework to stay in force despite authorizing the President pursuant to the AUMF. As a result, Congress's intent that FISA remain the statutory framework for electronic surveillance to collect foreign intelligence places the President's action in contravention to FISA's statutory framework and into the third category of the *Youngstown* framework.[377] The President's power would be at its lowest ebb and permissible only if the President retained the power exercised exclusive of the legislature.[378] Because war powers are shared and concurrent

---

marshall/crsreports/crsdocuments/RS2101701072005.pdf.

[370] *See id.* at 2.

[371] *Id.* at 2; *Church Hearings*, *supra* note 7, at ii.

[372] RELYEA, *supra* note 369, at 2.

[373] *See id.*; FISA 50 U.S.C. § 1811 (2000 & Supp. 2002).

[374] ACKERMAN & GRIMMETT, *supra* note 299, at 26–27. One of the key modern differences between formal declarations of war and authorizations of force is the fact that the latter does not trigger automatically standby statutory authorizations. *See id.* at 27.

[375] *See* BAZAN, *supra* note 117, at exsum.

[376] *See supra* notes 216–44 and accompanying text.

[377] *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637–38 (1952) (Jackson, J., concurring).

[378] *See id.*

between the President and Congress, the President's action fails the *Youngstown* test and is, therefore, unconstitutional.[379]

This conclusion is consistent with Justice Kennedy in his concurrence in *Hamdan* in which he specifically referred to the *Youngstown* test.[380] He pointed out that the President had no power to create a military tribunal as he acted in a field with a history of congressional involvement.[381] This legislative involvement sets a limit on presidential power. Kennedy stated,

> Where a statute provides the conditions for the exercise of governmental power, its requirements are the result of a deliberative and reflective process engaging both of the political branches. Respect for laws derived from the customary operation of the Executive and Legislative Branches gives some assurance of stability in time of crisis.[382]

V. THE NSA SURVEILLANCE VIOLATES THE FOURTH AMENDMENT

The Fourth Amendment consists of two clauses joined by the conjunction "and."[383] The first clause is a prohibition against unreasonable searches and seizures, and the second clause deals with the requirements for a warrant.[384] These warrant requirements include the justification required for the issuance of a warrant (probable cause) and the limitations on the scope of the warrant (particularity).[385] For much of the Fourth Amendment's history, the warrant clause was read in conjunction with the reasonableness clause so as to give meaning to the vague term "unreasonable."[386] Thus, in order for a search to be reasonable, it generally required probable cause and a warrant specifically describing its scope.

In recent years, the Supreme Court has abandoned this approach and has focused exclusively on the reasonableness clause without necessarily considering its relationship to the second warrant clause.[387] For example, in 2001, the Court in *United States v.*

---

[379] *See id.*

[380] Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2800 (2006) (Kennedy, J., concurring).

[381] *Id.*

[382] *Id.* at 2799.

[383] U.S. CONST. amend. IV.

[384] *Id.*

[385] *Id.*

[386] "Though the Fourth Amendment speaks broadly of 'unreasonable searches and seizures,' the definition of 'reasonableness' turns, at least in part, on the more specific commands of the warrant clause." United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 315 (1972) (citing United States v. Rabinowitz, 339 U.S. 56, 66 (1950)).

[387] *See generally* United States v. Knights, 534 U.S. 112 (2001) (focusing on the reasonableness of the "totality of circumstances" approach); New Jersey v. T.L.O., 469 U.S. 325 (1985) (finding that school officials do not need probable cause to search students so long as the search was reasonably related to the circumstances justifying the search).

Knights stated that "[t]he touchstone of the Fourth Amendment is reasonableness."[388] The decision in *Knights* built upon earlier holdings that recognized that "[t]he fundamental command of the Fourth Amendment is that searches and seizures be reasonable, and although 'both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search, . . . in certain limited circumstances neither is required.'"[389]

An early example of this approach can be found in the administrative search context. The Court encountered governmental searches in which traditional probable cause concepts requiring individual suspicion of wrongdoing did not work, such as housing code inspectors searching large areas for violations. In *Camara v. Municipal Court of San Francisco*, the Court turned to the reasonableness clause and devised a balancing approach to this issue.[390] The Court stated that "there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."[391] On one side of the balance, the Court weighed the governmental interest or need to conduct the particular type of Fourth Amendment activity.[392] On the other side of the balance, the Court looked to the intrusion that a particular search entailed.[393] This balance resulted in the validity of an administrative search adjudged by the reasonableness of its administrative regulations instead of the existence of probable cause.[394]

Initially, warrants were required for these administrative searches unless some exigency was present.[395] Over time, however, the Court began dispensing with the warrant requirement for heavily regulated businesses and when warrants would inhibit the inspections, with a limitation being the requirement that the regulations provide an adequate substitute for the particularity requirements of a warrant.[396]

The Court has expanded the administrative search rationale to include border searches,[397] drunk driving checkpoints,[398] and, by implication, airport searches.[399] One

---

[388] 534 U.S. at 118.

[389] *T.L.O.*, 469 U.S. at 340 (omissions in original) (quoting Almeida-Sanchez v. United States, 413 U.S. 266, 277 (1973) (Powell, J., concurring)).

[390] *See* 387 U.S. 523, 536–37 (1967).

[391] *Id.*

[392] *See id.* at 535.

[393] *See id.* at 538–39.

[394] *See id*. at 538 ("Having concluded that the area inspection is a 'reasonable' search of private property within the meaning of the Fourth Amendment, it is obvious that 'probable cause' to issue a warrant to inspect must exist if reasonable legislative or administrative standards for conducting an area inspection are satisfied with respect to a particular dwelling.").

[395] *See, e.g.*, *id.* at 535.

[396] *See, e.g.*, Donovan v. Dewey, 452 U.S. 594, 602–03 (1981) (upholding warrantless inspections required by the Mine Safety and Health Act); *see also* United States v. Biswell, 406 U.S. 311 (1972) (upholding warrantless inspections required by the Gun Control Act of 1968).

[397] United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

[398] Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

[399] *See* Chandler v. Miller, 520 U.S. 305, 323 (1997).

important limitation to keep in mind is that these searches are upheld because their purpose is something other than the general crime control objectives. For example, in *City of Indianapolis v. Edmond*, the Supreme Court refused to allow police checkpoints to interdict narcotic traffic because the principal purpose of the checkpoint was to detect evidence of criminal wrongdoing.[400]

Also evolving from the administrative search rationale is a subcategory often referred to as "special needs" situations. Justice Blackmun, in a concurring opinion in a high school search case, referred to this subcategory as applying when "special needs, beyond the normal need for law enforcement, make the warrant and [/or] probable-cause requirement[s] impracticable."[401] Reasonableness is ensured in these situations by limiting the discretion of the governmental officials involved and requiring a situation in which obtaining a warrant would simply not be practical.[402] For example, the Court in *New Jersey v. T.L.O.* stated, "The warrant requirement, in particular, is unsuited to the school environment: requiring a teacher to obtain a warrant . . . would unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools."[403] These "special needs" categories have allowed for warrantless and suspicionless Fourth Amendment activity in situations such as public school searches,[404] public employee searches,[405] and searches of people on probation.[406]

It is through the utilization of general reasonableness balancing and the "special needs" administrative approach that the Bush administration seeks to justify its warrantless NSA surveillance program.[407] The administration argues that the surveillance satisfies the Fourth Amendment and its requirement for reasonableness because the balance of the governmental interest in protecting against a terrorist attack outweighs

---

[400] 531 U.S. 32, 47–48 (2000).

[401] New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

[402] *See* Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 663–65 (1995) (upholding suspicionless and warrantless drug testing because it provides an administrative process with a minimal amount of discretion); Schmerber v. California, 384 U.S. 757, 770–71 (1966) (holding a warrantless blood alcohol content search reasonable due to blood's rapid loss of its alcohol content); *see also Edmond*, 531 U.S. at 54 (Rehnquist, C.J., dissenting) ("The 'special needs' doctrine . . . is an exception to the general rule that a search must be based on individualized suspicion of wrongdoing."); *Vernonia Sch. Dist.*, 515 U.S. at 661 ("It is a mistake, however, to think that the phrase 'compelling state interest,' in the Fourth Amendment context, describes a fixed, minimum quantum of governmental concern, so that one can dispose of a case by answering in isolation the question: Is there a compelling state interest here?").

[403] 469 U.S. at 340.

[404] *See id.* at 341–42.

[405] O'Connor v. Ortega, 480 U.S. 709, 721–25 (1987) (plurality opinion) (work-related searches of employees' desks and offices).

[406] Griffin v. Wisconsin, 483 U.S. 868, 876 (1987).

[407] *See* DOJ WHITE PAPER, *supra* note 24, at 37–39.

the resulting intrusion on privacy interests.[408] It is doubtful that the administration can argue credibly that the narrow "special needs" exception applies in this case.

A. Administrative Searches and the Reasonableness Balancing Approach

In balancing the governmental interest with the intrusion, certain factors should be considered. On the governmental interest side, the purpose of the search must not merely promote general crime control, but the method chosen must be narrowly tailored to advance that legitimate purpose.[409] On the intrusion side of the balance, one looks first to the nature of the privacy interest at stake and then to how the particular intrusion affects the privacy interest.[410] In addition, the degree of intrusion will be found to increase when the government officials enjoy a greater amount of discretion.[411]

The first issue to be resolved is whether the purpose of the NSA surveillance will serve a function other than normal general crime control purposes.[412] The government interest in the NSA surveillance searches, at first blush, appears to be rather compelling. The Bush administration characterizes the threat of terrorism as "not simply a matter of law enforcement," but a war that must be addressed by military means.[413] The mere gravity of the threat alone, however, does not resolve this issue.[414] The nature of the threat must be considered in relation to the law enforcement practices used to address the threat.[415]

When there is an imminent terrorist threat, the use of traditional law enforcement officials and procedures to address terrorism casts doubt on whether a clear distinction can be made between terrorism and general crime control.[416] The purpose of the warrantless NSA surveillance is to detect and prevent the death and destruction that

---

[408] *See id.*

[409] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 47–48 (2000); Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 652–54 (1995).

[410] *See Vernonia Sch. Dist.*, 515 U.S. at 654, 658.

[411] *See id.* at 663–64.

[412] *See Edmond*, 531 U.S. at 47–48.

[413] Dec. 19, 2005 Press Conference, *supra* note 3, at 1885.

[414] *See Edmond*, 531 U.S. at 42.

[415] *See* Delaware v. Prouse, 440 U.S. 648 (1979) (refusing to sanction random car stops for safety violations because the intrusion was great and the method utilized was not particularly effective given the intrusion).

[416] The legislative history for the passage of FISA recognizes the difficulty of drawing this distinction. When surveillance targets U.S. persons, the Senate recognized that "[i]ntelligence and criminal law enforcement tend to merge." S. REP. NO. 95–701, at 11 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3979. The distinction becomes even harder once it is pointed out that the United States has addressed terrorist acts through traditional law enforcement means in the past; this includes the bombings of the U.S. Embassy in Nairobi and the Oklahoma City bombing. *See* M. Wood, *U.S. Struggling to Make Law Enforcement, Military Models Handle Detainees, Terror Suspects*, Forum at U. Va. (Nov. 16, 2005), *available at* http://www.law.virginia.edu/home2002/html/news/2005_fall/terrorforum.htm.

comes from attacks on American people and infrastructure.[417] It is difficult, if not impossible, to determine how a car bomb detonated by an Al Qaida operative is distinguishable from a car bomb detonated by a domestic criminal. In 2002, the United States Foreign Intelligence Surveillance Court of Review, in *In re Sealed Case*, recognized that this distinction is especially difficult when attempting to justify foreign intelligence collection of a United States person under the FISA definition of an "agent of a foreign power."[418] The court noted that "the definition of an agent of a foreign power—if he or she is a U.S. person—is grounded on criminal conduct."[419] The warrantless NSA surveillance includes domestic citizens and places; therefore, it falls within conduct closely associated with criminal activity.[420] Upholding a warrantless search to effectuate this purpose would constitute an expansion of the Supreme Court's narrow "special needs" cases to include searches that employ law enforcement officials in a manner similar to crime control.[421]

The "special needs" exception also requires a narrowly tailored nexus between the governmental purpose and the means used to effectuate that purpose.[422] Justice Scalia, in his dissent in *National Treasury Employees Union v. Von Raab*, highlights the nexus requirement by distinguishing the programmatic search at issue from the special needs search in *Skinner v. Railway Labor Executives Association*.[423] In *Skinner*, a case involving employee drug tests immediately following a railroad accident, the Court upheld the ability to drug test railroad employees due to the demonstrated effects that drugs and alcohol have had on the safety of railroad operations.[424] Justice Scalia distinguished the nexus that existed in *Skinner* from the justification provided in *Von Raab* that sought to administer drug tests to customs officials who were being considered for promotion.[425] In *Von Raab,* the urine testing sought to protect the integrity of the Customs Service by discharging employees who, due to their own drug use, may be unsympathetic to their duty to interdict narcotics.[426] Justice Scalia argued that the nexus presented was too generalized and speculative and could not support a finding of reasonableness.[427]

The requirement of a nexus between the purpose and the means employed basically speaks to the need for a narrowly tailored program when operating outside the warrant

---

[417] *See* Dec. 19, 2005 Press Conference, *supra* note 3, at 1885.

[418] 310 F.3d 717, 723 (FISA Ct. Rev. 2002).

[419] *Id.*

[420] *See id.*; Risen & Lichtblau, *supra* note 6.

[421] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 47–48 (2000).

[422] *See* Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 680–81 (1989) (Scalia, J., dissenting); Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 629–30 (1989).

[423] *See* 489 U.S. at 680–81 (Scalia, J., dissenting).

[424] *Id.* at 684; *see Skinner*, 489 U.S. at 608.

[425] *See Von Raab*, 489 U.S. at 680–82 (Scalia, J., dissenting).

[426] *Id.* at 682.

[427] *See id.* at 684.

requirement.[428] The Bush administration argues that the warrantless electronic surveillance is narrowly tailored to prevent terrorist attacks because the program is only targeted at individuals who are reasonably believed to be associated with Al Qaida.[429] There are no indications, however, that such a program can discriminate to the necessary degree.[430] The sparse information released so far on the details of the program appears to speak to the opposite conclusion.[431] There are indications that hundreds and maybe thousands of Americans have been targeted by this warrantless surveillance.[432] The flexibility, vagueness, and discretion that a definition of a supporter or associate of Al Qaida entails—which could conceivably include charitable contributions to innocuous religious organizations—demonstrates how expansive and unguided the application of such a vast collection program could be when motivated to prevent a general terrorist attack.[433] In addition, one factor that drove the Church Committee to recommend what would become FISA was the inability for NSA to discriminate among proper and improper targets.[434]

Even if it is possible for the NSA to discriminate accurately between proper and improper targets, the core question is whether the electronic surveillance could properly identify information indicating an imminent terrorist attack.[435] The Bush administration cites dicta in *Edmond* that implies that a warrantless and suspicionless roadblock would be permissible if employed to "thwart an imminent terrorist attack."[436] This dicta demonstrates, however, not that stopping a terrorist attack automatically justifies a traffic roadblock but that a roadblock may, in a situation when an imminent attack looms, provide a narrowly tailored means to address that threat.[437] Similarly, electronic surveillance may not always lack the adequate nexus when indications of an imminent terrorist attack require immediate use of the technology, but the program's four year duration suggests its use more as a general intelligence tool rather than a narrowly tailored means to address ripe threats.[438]

---

[428] *See* Delaware v. Prouse, 440 U.S. 648, 659 (1979) (holding that random spot checks were not narrowly tailored to the purpose of ensuring an adequate amount of insurance coverage); *see also* Chandler v. Miller, 520 U.S. 305, 309 (1997) (labeling the category of constitutionally permissible suspicionless searches as "closely guarded").

[429] DOJ WHITE PAPER, *supra* note 24, at 40.

[430] Dec. 19, 2005 Press Conference, *supra* note 3, at 1889.

[431] *See id.*

[432] *See* Risen & Lichtblau, *supra* note 6.

[433] *See id.* (noting that intelligence officials have eavesdropped on people in the United States who are linked indirectly to suspected terrorists).

[434] *See Church Hearings*, *supra* note 7, at 37–38 (statement by Sen. Walter Mondale).

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

[436] *See id.*

[437] *See id.*

[438] *See id.*; Risen & Lichtblau, *supra* note 6; *see also* Delaware v. Prouse, 440 U.S. 648, 659 n.18 (1979) (explaining that officers at a roadblock could permissibly search for stolen cars but only if the search could be narrowly tailored to address a highway safety need such as a high-speed getaway, not the general interest in stolen vehicles).

In analyzing the intrusion, this situation involves a search of ordinary persons and of information that often emanates from the home—a place of heightened privacy expectation.[439] This situation differs from an intrusion on school children or on employees in the heavily regulated railroad industry whose privacy expectation is lessened.[440] Further, the Court has long recognized the intrusiveness of wiretap information, which further increases the weight on the intrusion side of the reasonableness test balance.[441]

A further factor to consider in analyzing the intrusion is the amount of discretion afforded law enforcement. The standardized nature of programs that satisfy the "special needs" exception do not simply distinguish the governmental purpose from general crime control, but they provide additional safeguards that address the same concerns about arbitrary intrusion on privacy that normally drive the warrant requirement.[442] For instance, the Supreme Court, in *Vernonia School District v. Acton,* held a drug testing program for all student athletes permissible under the "special needs" exception to the Fourth Amendment partly because the mandatory nature of the search, rather than random drug testing, makes the program less susceptible to arbitrary application.[443] An analogous principle is evident in the Supreme Court's willingness to uphold warrantless and suspicionless inventory searches when standardized criteria restrict the exercise of discretion of the government official conducting the search.[444]

These safeguards are relied upon and held sufficient to protect privacy interests because they detach the determination of the need for a search from those charged with administering it.[445] In this manner, standardized policies serve the equivalent function of a neutral magistrate in a traditional warrant process.[446]

---

[439] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.").

[440] Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 656 (1995) ("Fourth Amendment rights . . . are different in public schools than elsewhere . . . ."); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 620 (1989) (detailing the heavily regulated nature of the railroad industry and railroad employees).

[441] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

[442] *See Skinner*, 489 U.S. at 622 (explaining that the purpose of a warrant requirement is to ensure than an objective determination is made as to whether an intrusion is justified).

[443] *See* 515 U.S. at 663–64; *see also Skinner*, 489 U.S. at 622 (holding drug testing of railroad employees permissible because "the circumstances justifying toxicological testing and the permissible limits of such intrusions are defined narrowly and specifically in the regulations that authorize them").

[444] *But see* Florida v. Wells, 495 U.S. 1, 3–4 (1990) (holding an inventory search impermissible because in the absence of a policy specifically requiring the opening of closed containers, the government official's decision to do so constituted the exercise of too much discretion).

[445] *See Skinner*, 489 U.S. at 622.

[446] *See id.*

United States v. U.S. District Court (*Keith*) remains the only case in which the Supreme Court addressed the use of wiretaps for national security purposes.[447] In holding that electronic surveillance for domestic security, even in light of national security imperatives, requires a warrant, the Court went on to say that "[t]hese Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[448] Justice Douglas, in his concurrence, went even further and stated that given "the clandestine nature of electronic eavesdropping," the government bears a heavy burden to show why a warrantless search is necessary.[449] He went on to say that

> [t]he Warrant Clause has stood as a barrier against intrusions by officialdom into the privacies of life. But if that barrier were lowered now to permit suspected subversives' most intimate conversations to be pillaged then why could not their abodes or mail be secretly searched by the same authority? To defeat so terrifying a claim of inherent power we need only stand by the enduring values served by the Fourth Amendment.[450]

The Bush administration argues that periodic review and individual authorization of the warrantless NSA electronic surveillance by the President and the Attorney General provides the safeguards necessary to satisfy the Fourth Amendment.[451] This presents a system of authorization in which the discretion as to whether and to what extent to conduct a search is fused with those in charge of administering the program.[452] The electronic surveillance program, therefore, does not contain any of the additional safeguards that serve to justify dispensing with the warrant process and the intervention of a neutral magistrate.[453]

Thus, even though the important governmental interest at stake is recognized, there is uncertainty whether the objectives of this interest would be served by the NSA surveillance. Additionally, even if the surveillance did advance the purpose to some extent, the scope of the intrusion coupled with the unbridled discretion of the executive presents a program unlikely to pass Fourth Amendment muster.

---

[447] *See generally* 407 U.S. 297 (1972) (addressing the constitutionality of wiretaps for domestic surveillance).

[448] *Id.* at 316–17.

[449] *Id.* at 324–25 (Douglas, J., concurring).

[450] *Id.* at 332.

[451] *See* Dec. 19, 2005 Press Conference, *supra* note 3, at 1889.

[452] *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 622 (1989); Risen & Lichtblau, *supra* note 6.

[453] *See* Vernonia Sch. Dist. v. Acton, 515 U.S. 64, 663–64 (1995).

B. Administrative Searches and the Impracticability of Warrants Approach

The second category of "special needs" cases recognized by the Supreme Court entails circumstances in which obtaining a warrant would be impracticable.[454] These cases generally involve emergency situations in which obtaining a warrant would result in the destruction of the evidence or in which unique circumstances exist that counsel against the traditional warrant process.[455] Typical examples include the *Skinner* case, in which requiring a warrant to obtain drug tests after an accident would have resulted in the loss of the evidence due to the body's rapid elimination of alcohol,[456] and *T.L.O.*, in which requiring a school official, who was attempting to maintain school rules and discipline, to first obtain a warrant would simply be impracticable.[457]

Despite its more forgiving requirements for permissible governmental purposes, the "special needs" emergency exception does not justify the NSA surveillance because a practical warrant process exists to address the particular needs of this surveillance.[458] Congress passed FISA to provide a warrant process adapted to the sensitive and flexible needs of electronic surveillance of foreign intelligence.[459] In addition, Congress included an emergency exception to this general warrant process to address situations in which the Attorney General reasonably believes that the gravity and expediency of the need prohibits prior judicial notification.[460] The emergency exception to FISA appears to address statutorily the "special needs" exception in the context of electronic surveillance for foreign intelligence.[461] FISA allows for such an exception to apply but takes away discretion as to its scope and duration by placing statutory limits on them.[462]

The explicit FISA emergency exception suggests that no "special needs" exception would be applicable to electronic surveillance in nonconformance with those limits.[463]

---

[454] *See* Camara v. Municipal Ct. of San Francisco, 387 U.S. 523, 533 (1967) (recognizing that the justification for the government to dispense with the warrant requirement is strongest when "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search").

[455] *See, e.g.*, Schmerber v. California, 384 U.S. 757, 770 (1966) (upholding a search to prevent the destruction of evidence of intoxication).

[456] *Skinner*, 489 U.S. at 623.

[457] New Jersey v. T.L.O., 469 U.S. 325, 340 (1985).

[458] *See* FISA, 50 U.S.C. § 1805(f) (2002) (providing the Attorney General the ability to employ electronic surveillance in emergency situations for seventy-two hours with only retroactive judicial approval); *Camara*, 387 U.S. at 533.

[459] *See* S. REP. NO. 95–604, pt. 1, at 5 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3906 ("The purpose of the bill is to provide a procedure under which the Attorney General can obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.").

[460] *See* FISA, 50 U.S.C. § 1805(f); S. REP. NO. 95–701, at 57 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 4026.

[461] *See* FISA, 50 U.S.C. § 1805(f).

[462] *See id.*

[463] *See id.*

The Bush administration admits that the warrantless NSA surveillance did not comply with the requirements listed in FISA.[464] Thus, with a practical and obtainable warrant process, the justification for the surveillance based upon a "special needs" exception would unduly expand the doctrine past its judicially constructed limits and divorce it from the exigency that supports dispensing with the traditional warrant requirement.[465]

In addition, the Supreme Court has been willing to dispense with the warrant requirement in these "special needs" situations because the existence of standardized and discretionless criteria makes evaluation by a neutral magistrate unnecessary and practically worthless.[466] For example, in *Vernonia*, the program at issue required drug testing for every student wishing to participate in athletics.[467] The procedures for gathering the urine and conducting the drug test were carefully limited to reduce the intrusion and to reduce discretion.[468] The test results were distributed "only to a limited class of school personnel" and not otherwise used for internal school discipline.[469] The Court found these standards sufficient to reduce the discretion of the officials to a degree in which no facts leading to suspicion would exist for a neutral magistrate to evaluate.[470] There is no indication at this point that the warrantless NSA surveillance was conducted in such a discretion-less manner. In fact, all indications appear to suggest that the program was administered based on individual suspicion and not standardized criteria.

C. Administrative Border Searches

One last possible Fourth Amendment justification for the NSA searches would be to compare them to administrative border searches. Historically, these searches have been justified by the "longstanding right of the sovereign to protect itself" from dangerous people or things entering the country.[471] Since the attacks on September 11, the Supreme Court has shown a willingness to expand the scope of such searches.[472] For example, the Court recently allowed for the total disassembly and detention for nearly an hour of an automobile that sought to cross into the United States.[473]

---

[464] *See* Dec. 19, 2005 Press Conference, *supra* note 3, at 1887; *see also* Risen & Lichtblau, *supra* note 6.

[465] *See* Camara v. Municipal Ct. of San Francisco, 387 U.S. 523, 533 (1967); Schmerber v. California, 384 U.S. 757, 770–71 (1966).

[466] *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 622 (1989).

[467] *See* Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 663–64 (1995).

[468] *Id.* at 658–59.

[469] *Id.* at 658.

[470] *See id.* at 664–65; *see also Skinner*, 489 U.S. at 622 ("[I]n light of the standardized nature of the tests and the minimal discretion vested in those charged with administering the program, there are virtually no facts for a neutral magistrate to evaluate.").

[471] United States v. Ramsey, 431 U.S. 606, 616 (1977).

[472] *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 154 (2004) (expanding the scope of border searches to include the removal of gas tanks).

[473] *See id.*

The argument to include the NSA surveillance as a border search would be that the information is emanating from a foreign source and is crossing our borders reaching computers here in the United States. Although the Supreme Court has never addressed this particular issue, there is some support for this proposition.[474]

In 1977, in *United States v. Ramsey*, the Supreme Court upheld the opening of eight envelopes at the international border.[475] The Court noted, however, that the search was limited to determining whether the envelopes contained something other than correspondence.[476] The border officials were not allowed to read any correspondence that may have been inside the envelopes.[477]

The distinction drawn by the Court in *Ramsey* between items and correspondence is critical and likely dispositive on the NSA surveillance issue.[478] The justification for the border search exception is grounded in the recognized right of the sovereign to control "who and what may enter the country."[479] Just as the "what" in *Ramsey* did not include the reading of correspondence, it also does not include correspondence intercepted by electronic surveillance.[480]

CONCLUSION

The revelation of the warrantless electronic surveillance program conducted by the Bush administration was met with criticism across a spectrum of the public. The general public, unfamiliar with the intricacies of FISA and the constitutional power aspects of the issue, intuitively felt an abuse of power. Constitutional scholars agreed but were even more shocked by the clarity and brazen nature of the illegality.[481]

The Bush administration responded to the criticism with a comprehensive response that argued every front of the gathering legal battle.[482] The comprehensive nature of the legal response, however, underscored the insincerity of the justifications proffered because it implied an almost self-evident clarity to arguments that, at best, were grasping for threads of authority.

Despite the numerous constitutional justifications provided by the President, the argument for permissibility boils down to a reliance on the need to fight the "war on

---

[474] *See Ramsey*, 431 U.S. at 624 (upholding the search of letters at a border crossing); United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) (upholding the search of the contents of a computer at the border).

[475] 431 U.S. at 624–25.

[476] *Id.* at 624.

[477] *Id.*

[478] *See id.*

[479] *See id.* at 620.

[480] *See id.* at 620, 624.

[481] *See generally* Cole et al., *supra* note 115 (providing a letter to Congress signed by fourteen prominent constitutional law scholars and former government officials).

[482] *See generally* DOJ WHITE PAPER, *supra* note 24.

terrorism" through any means possible.[483] Opposing the exercise of this unchecked discretion over technology as powerful as the NSA yields does not require a finding of poor motive by the President. There is little doubt that the President genuinely feels that the warrantless surveillance will help prevent additional attacks on the nation's homeland. The point is that this determination is not his alone to make.

History is replete with examples of inflated executive claims for necessary restrictions on constitutional rights under threat of imminent danger.[484] Examples include the internment of Japanese-Americans, the summary military tribunal process and execution of German saboteurs during World War II, and the suspension of the writ of *habeas corpus* in the Civil War.[485] In each of these cases, the nation and the Supreme Court abstained from restricting the immense power assumed by the President, and these excesses are looked upon in retrospect through embarrassed and critical lenses.[486]

Yet, as if inevitable, a similar executive assertion of power surfaces once again. Perhaps most shocking about the modern abuse is the similarity it shares with those associated with former President Richard M. Nixon—experiences within the political memory of the politicians and executive branch bureaucrats currently in power. The repetition of history's mistakes is understandable, though still not pardonable, when based upon ignorance of the past. It is condemnable, however, to repeat mistakes based on an arrogant refusal to learn from them.

Of course, there may be some truth to an argument that warrantless surveillance will increase the government's ability to protect against a terrorist attack. It is mere speculation to determine the operational effectiveness of bypassing a court order process. But even if there is some advantage, the real question is at what cost is this advantage obtained.[487] Israel's Chief Justice of the Supreme Court, Aharon Barak, addressed and answered this same balancing of security and humanitarian interests in 2004 when ordering the Israeli army to remove a portion of the West Bank Security Wall due to its burden on the Palestinians.[488] Justice Barak's words suggest

---

[483] *See* Dec. 19, 2005 Press Conference, *supra* note 3, at 1885 ("To save American lives, we must be able to act fast and to detect these conversations so we can prevent new attacks.").

[484] *See* David Rudovsky, *The Impact of the War on Drugs on Procedural Fairness and Racial Equality*, 1994 U. CHI. LEGAL F. 237, 238–39.

[485] *Id.*; *see also* FISHER, *supra* note 290, at 205–08 (quoting Justice Felix Frankfurter, who sat on the Supreme Court when it decided *Ex parte Quirin*, as stating it "was not a happy precedent").

[486] *See* Rudovsky, *supra* note 484, at 239.

[487] A Task Force on Domestic Surveillance in the Fight Against Terrorism was appointed by American Bar Association (ABA) President Michael S. Greco. The task force included a former FBI director and former General Counsel to the CIA and NSA. The ABA House of Delegates adopted the recommendations of the task force at the midyear meeting (Feb. 2006). One of the adopted recommendations states that the ABA is opposed to any electronic surveillance inside the United States by the government "for foreign intelligence purposes that does not comply with" FISA. ABAnet.org, Task Force on Domestic Surveillance in the Fight Against Terrorism, http://www.abanet.org/op/domsurv (last visited Aug. 23, 2006).

[488] Gareth Evans, President, Int'l Crisis Group, Lecture at the University of New South

an acknowledgment that to win the war may be a Pyrrhic victory if individual liberties are sacrificed in its wake:

> We are aware that in the short term, this judgment will not make the state's struggle against those rising up against it any easier . . . This is the destiny of a democracy: she does not see all means as acceptable, and the ways of her enemies are not always open before her. A democracy must sometimes fight with one arm tied behind her back. Even so, democracy has the upper hand. The rule of law and individual liberties constitute an important aspect of her security stance.[489]

The Constitution, of course, is not a suicide pact,[490] but it does provide the wax and rope to block and bind the passions and fears of the moment. If this nation is to sail past the Sirens' song of terrorism and fear, it must do so with renewed dedication to our first principles and to the liberties and democratic ideals that make our society worth the fight.

POSTSCRIPT

On July 26, 2006, the Senate Judiciary Committee held hearings to consider legislation that would deal with the NSA surveillance discussed in this article.[491] General Michael Hayden, director of the Central Intelligence Agency, presented legislation developed by Senator Arlen Specter, Chair of the Judiciary Committee, and the President.[492] The proposal would allow the FISC to review the administration's program of warrantless monitoring of international communication as opposed to individual warrant and determine its constitutionality.[493] The Spector-White House proposal would rely on the President to seek voluntarily judicial review. Further, if review was denied, the President would have the right to appeal or resubmit the proposal until such time as it receives approval by the FISC. This procedure would

---

Wales, Sydney: The Global Response to Terrorism 10 (Sept. 27, 2005), *available at* http://www.unsw.edu/au/news/pad/articles/2005/sep/FINALWurthLectureTerrorismGE.pdf.

[489] *Id.*; *see also* Michael S. Greco, *A False Choice: The American People Should Not Be Forced to Choose Between Freedom and Security*, 92 A.B.A. J. 6 (2006) ("The president has a sacred obligation under the Constitution to protect both the nation's safety and its constitutionally-guaranteed freedoms—and to honor the doctrine of separation of powers. His failure to do so would compromise the very principles and ideals that we are fighting to protect.").

[490] Though this term is often attributed to President Abraham Lincoln, the first known written reference appears in Justice Jackson's dissent in *Terminiello v. Chicago*, 337 U.S. 1, 37 (1949).

[491] *See* Eric Lichtblau, *Administration and Critics, in Senate Testimony, Clash over Eavesdropping Compromise*, N.Y. TIMES, July 27, 2006, at A21.

[492] *See id.*

[493] *Id.*

eliminate the need to review individual warrants and would largely make the FISA procedure, enacted almost thirty years ago, a nullity.[494]

This procedure is reminiscent of colonial times when custom officers armed with writs of assistance could search anywhere they pleased. These writs were issued without probable cause, without any specificity with regard to things to be seized or places to be searched, and were in effect until six months after the death of the reigning monarch. These writs provided the impetus for our founding ancestors as they developed the Fourth Amendment.[495] As a matter of fact, in the Massachusetts colonial court there was a petition by a customs officer for a new writ of assistance after the death of King George II. James Otis, appearing on behalf of the inhabitants of Boston, made such an eloquent argument that it moved a young John Adams, one of the signers of the Declaration of Independence, who described the argument fifty-six years later as follows: "Otis was a flame of Fire! . . . Then and there was the first scene of the first Act of Opposition to the arbitrary Claims of Great Britain. Then and there the child Independence [sic] was born."[496] The administration's proposal is nothing more than a modern day writ of assistance.

On September 28, 2006, the United States House of Representatives by a vote of 232 to 191 approved legislation that would give the President the power to order wiretaps for up to ninety days without a court order. The United States Senate is not likely to address the bill until after the November election.[497] The Senate's approach of submitting the entire surveillance program to the FISC or the House's approach of ninety days wiretaps without a court order present a clear signal of more expansive presidential power to conduct warrantless surveillance of American citizens. How this legislation will affect or be affected by ongoing judicial review of the warrantless surveillance program remains to be seen.[498]

---

[494] *See id.*

[495] *See* Robert M. Bloom, *Warrant Requirement—The Burger Court Approach*, 53 U. COLO. L. REV. 691, 694 (1982).

[496] LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 157 (1999).

[497] *See* Eric Lichtblau, *House Approves Power for Wiretaps Without Warrants*, N.Y. TIMES, Sept. 29, 2006, at A18.

[498] *See* ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *stay granted by* 2006 WL 2827166 (6th Cir. Oct. 4, 2006).