HOW THE USA PATRIOT ACT WILL PERMIT GOVERNMENTAL INFRINGEMENT UPON THE PRIVACY OF AMERICANS IN THE NAME OF "INTELLIGENCE" INVESTIGATIONS

SHARON H. RACKOW[†]

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[1]

In the wake of September 11, 2001, as Americans watched time and again the news footage of airplanes crashing into the World Trade Center in New York City, many resolved to support the Bush administration in its efforts to find the terrorists responsible for those horrific actions and bring them to justice—at whatever cost necessary. Mourning the loss of so many lives, and faced with warnings of additional terrorist attacks, Americans called for legislative action in the hope that new laws would grant the government sufficient surveillance capabilities to catch terrorists hiding on U.S. soil, thereby leading to greater security at home. "An ABC-*Washington Post* poll taken the day after September 11th found that two out of three Americans are willing to surrender civil liberties to stop terrorism."[2]

Private citizens were not alone in their desire for legislative reform. Immediately after September 11th, the Bush administration advocated radical amendments to existing law to allow intelligence and

---

[†] B.A. 1998, Williams College; J.D. Candidate 2003, University of Pennsylvania. Many thanks to my colleagues on the *University of Pennsylvania Law Review* for their insightful suggestions and excellent editing skills. I am grateful to Professor David Rudovsky for providing invaluable advice on early drafts of this Comment. Thank you to James Matthews for his guidance. I would be remiss if I did not mention those who have been my cheering section throughout this process: Thank you to my family (Mom, Dad, and Beth) for your love and encouragement throughout all my endeavors—with a special thanks to my Dad, for diligently helping me to hone my writing style. And to Christopher Herrick, thank you for your unyielding support and confidence. This Comment is dedicated to all those who perished in the attacks of September 11, 2001. Your memories live on in all our hearts—you will not be forgotten.

[1] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

[2] Brigid McMenamin, *Land of the Free*, FORBES, Oct. 15, 2001, at 56.

law enforcement agencies access to the essential tools[3] required to uncover terrorist activity in the United States. As the House of Representatives and Senate began to debate the proposals promoted by Attorney General John Ashcroft, concerns emerged regarding the extent to which these new provisions would infringe upon cherished civil liberties. As the House's Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("PATRIOT Act")[4] and the Senate's comparable Uniting and Strengthening America Act of 2001 ("USA Act")[5] began to take shape under the Bush administration's "'relentless' pressure to move quickly, 'without deliberation or debate,'"[6] it became apparent that several provisions of the bills would permit the government to intrude upon the private lives of law-abiding Americans—without assurance of any greater security against terrorism. The American Civil Liberties Union expressed its view in a letter to the Senate, commenting that:

> While it contains provisions that we support, the American Civil Liberties Union believes that the USA PATRIOT Act gives the Attorney General and federal law enforcement unnecessary and permanent new powers to violate civil liberties that go far beyond the stated goal of fighting international terrorism. These new and unchecked powers could be used against American citizens who are not under criminal investigation, immigrants who are here within our borders legally, and also against those whose First Amendment activities are deemed to be threats to national security by the Attorney General.[7]

Despite such concerns, on October 26, 2001, President George W. Bush signed the House and Senate's compromise antiterrorism bill, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

---

[3] During the time that the House and Senate were creating what would become the USA PATRIOT Act, "Attorney General John D. Ashcroft characterized the anti-terrorism bill as a package of 'tools' urgently needed to combat terrorism." Jim McGee, *An Intelligence Giant in the Making—Anti-Terrorism Law Likely to Bring Domestic Apparatus of Unprecedented Scope*, WASH. POST, Nov. 4, 2001, at A4.

[4] H.R. 2975, 107th Cong. (2001).

[5] S. 1510, 107th Cong. (2001).

[6] Adam Clymer, *Bush Set to Sign*, N.Y. TIMES, Oct. 26, 2001, at A1 (quoting Sen. Feingold); *see also* 147 CONG. REC. S10,366 (daily ed. Oct. 9, 2001) (statement of Sen. Leahy) ("We have expedited the legislative process in the Judiciary Committee to consider the administration's proposals. In daily news conferences, the Attorney General has referred to the need for such prompt consideration.").

[7] Letter from Laura W. Murphy, Director, ACLU Washington Office, and Gregory T. Nojeim, Associate Director & Chief Legislative Counsel, ACLU, to the United States Senate (Oct. 23, 2001), *available at* http://www.aclu.org/congress/l102301k.html.

("USA PATRIOT Act").[8]

One multifaceted aspect of the USA PATRIOT Act that has received a great deal of criticism from both civil libertarians and the press alike is the broad expansion of the government's right to engage in electronic surveillance. This Comment addresses how three discrete provisions of the Act allow the government far greater power to: (1) monitor the private telephone conversations of individuals suspected of purely domestic criminal activity, without demonstrating probable cause that a crime has been or is soon to be committed, under the guise of an "intelligence" investigation; (2) overhear private conversations of nonsuspects permitted by the extension of roving wiretap authority to foreign intelligence investigations without proper privacy protections; and (3) discourage political dissent by including the activities of unpopular political organizations within the newly created definition of "domestic terrorism."

By enacting these three provisions, the USA PATRIOT Act disrupts the delicate inherent in our established surveillance laws,[9] which prior to September 11th provided the government with sufficient leeway to conduct both criminal and intelligence surveillance while protecting Americans' Fourth and First Amendment rights to be free from "unreasonable searches and seizures"[10] and to exercise freedom of expression.[11] Through a review of Fourth and First Amendment rights, an analysis of pre-USA PATRIOT Act surveillance law, and a discussion of how three provisions of the USA PATRIOT Act greatly increase the government's surveillance abilities, this Comment illustrates how the USA PATRIOT Act allows the government to compromise cherished freedoms the American people[12] both enjoy and celebrate as part of our national identity.

---

[8] H.R. 3162, 107th Cong. (2001) (enacted).

[9] Omnibus Crime Control and Safe Streets Act of 1968, tit. III, 18 U.S.C. §§ 2510-2520 (1994); Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811 (1994).

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

[11] U.S. CONST. amend. I.

[12] The USA PATRIOT Act affects the rights of United States citizens and noncitizens differently, a distinction which is beyond the scope of this Comment. Therefore this Comment focuses exclusively on how the Act infringes on American citizens' Fourth and First Amendment rights.

I. REVIEW OF FOURTH AND FIRST AMENDMENT RIGHTS

A. *The Fourth Amendment*

The strongest protection Americans have against governmental intrusions into their privacy interests is the Fourth Amendment, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[13] Early interpretations of the Amendment tended toward a literal and narrow reading of the wording, such that it protected only physical property interests. An example of this property-based application is *Boyd v. United States*, in which the Court found that compelled production of a person's private papers constituted an unreasonable search and seizure within the meaning of the Fourth Amendment.[14] To reach this conclusion, the Court heavily relied upon the English case of *Entick v. Carrington*,[15] finding Lord Camden's pronouncement of the judgment to be "sufficiently explanatory of what was meant by unreasonable searches and seizures."[16] In *Entick*, the English court stated that:

> Papers are the owner's goods and chattels; they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.[17]

The *Boyd* Court reasoned that "[i]t is not the breaking of [a man's] doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and *private property* . . . which underlies and constitutes the essence of Lord Camden's judgment."[18]

---

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

[14] 116 U.S. 616, 634-35 (1886). The property rights conception of the Fourth Amendment is clearly abrogated by current jurisprudence after the *Katz v. United States* decision, discussed *infra* notes 23-26 and accompanying text.

[15] 95 Eng. Rep. 807 (K.B. 1765), *in* 19 HOWELL'S STATE TRIALS 1029.

[16] *Boyd*, 116 U.S. at 627. "As every American statesman . . . was undoubtedly familiar with this monument of English freedom, and considered it as the true and ultimate expression of constitutional law, it may be confidently asserted that its propositions were in the minds of those who framed the Fourth Amendment to the Constitution . . . ." *Id.* at 626-27.

[17] 95 Eng. Rep. 807 (K.B. 1765), *in* 19 HOWELL'S STATE TRIALS 1029; *see also Boyd*, 116 U.S. at 627-28 (quoting this passage in full).

[18] *Boyd*, 116 U.S. at 630 (emphasis added).

Property notions also controlled cases concerning electronic surveillance such as *Olmstead v. United States*, in which the Court ruled that the wiretap in question did not violate the appellant's Fourth Amendment rights.[19] The Court reasoned that there could be no search when there was no physical invasion of the appellant's personal space, and likewise there could be no seizure considering that words are not tangible things capable of being seized.[20] Yet Justice Brandeis's dissent signaled a shift in attitude away from such unyielding property-based applications of the Fourth Amendment when he stated:

> The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone . . . . To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[21]

In describing the right conferred by the Fourth Amendment as the right "to be let alone," Justice Brandeis was referring to the influential article he had written with Samuel D. Warren, entitled *The Right to Privacy*, which argued for common law recognition of a fundamental right to privacy.[22]

Thirty-nine years after *Olmstead*, the Court again faced an electronic surveillance controversy in *Katz v. United States*, in which FBI agents—acting without a warrant—set up a wiretap by attaching a listening device to the outside of a public telephone booth from which the appellant was engaging in illegal bookmaking activities.[23] Influenced by notions of privacy, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[24] In a concurring

---

[19] 277 U.S. 438, 466 (1928).

[20] *See id.* at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

[21] *Id.* at 478 (Brandeis, J., dissenting).

[22] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

[23] 389 U.S. 347, 348 (1967).

[24] *Id.* at 353.

opinion, Justice Harlan created a two-part test to determine when the Fourth Amendment, which the Court declared "protects people, not places,"[25] actually confers such protection. Justice Harlan explained that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[26] This opinion, which was later accepted by a majority of the Court,[27] demonstrates a clear shift in the Court's interpretation of the protections afforded by the Fourth Amendment, away from property-based conceptions and toward privacy-based notions. Privacy as protected by the Fourth Amendment denotes a right to be free from unwarranted governmental surveillance, and such privacy interests should be kept in mind when considering the implications of the USA PATRIOT Act.

B. *The First Amendment*

Governmental surveillance also may infringe upon the First Amendment rights of Americans by chilling free expression, particularly in the context of political protest. The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech."[28] This explicit constitutional protection of expressive activity is upheld with particular vigor when individuals exercise this freedom as a means of political protest. While many forms of expressive activities are protected by the First Amendment, the courts have allowed little or no protection for those who seek to incite violence,[29] or who use violence or otherwise illegal acts as a means of protest.[30] As the Supreme Court declared in *NAACP v. Claiborne Hardware Co.*, "'violence has no sanctuary in the First Amendment, and the use of weap-

---

[25] *Id.* at 351.

[26] *Id.* at 361 (Harlan, J., concurring).

[27] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986) (restating and applying the test from Justice Harlan's concurrence in *Katz*).

[28] U.S. CONST. amend. I.

[29] *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam) ("[T]he constitutional guarantee[] of free speech . . . do[es] not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.").

[30] *See, e.g.*, Wisconsin v. Mitchell, 508 U.S. 476, 484 (1993) ("'[V]iolence or other types of potentially expressive activities that produce special harms distinct from their communicative impact . . . are entitled to no constitutional protection.'" (quoting Roberts v. United States Jaycees, 468 U.S. 609, 628 (1984))).

ons, gunpowder, and gasoline may not constitutionally masquerade under the guise of "advocacy."'"[31] Since violent or illegal acts are not protected under the right to free expression, the First Amendment will not act as a barrier against government surveillance of such activities. Yet, where individuals exercise free expression in a manner protected by the First Amendment, government surveillance may not be targeted specifically at such behavior.[32] Interests protected by the First and Fourth Amendments converge in this context, as intrusive surveillance activities discourage the exercise of protected expression.[33] In *United States v. United States District Court*, the Court stated that "[h]istory abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."[34] Thus, although the framers' motives in developing and passing the USA PATRIOT Act were almost certainly benevolent—in that they were seeking to safeguard national security and protect Americans from further terrorist attacks—it is important to consider carefully how the Act will permit government surveillance of targets exercising protected free expression.

II. PRE-USA PATRIOT ACT SURVEILLANCE LAW: TITLE III AND FISA

Prior to the enactment of the USA PATRIOT Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[35] and the Foreign Intelligence Surveillance Act of 1978 (FISA)[36] provided United States law enforcement and intelligence agencies exten-

---

[31] 458 U.S. 886, 916 (1982) (quoting Samuels v. Mackell, 401 U.S. 66, 75 (1970) (Douglas, J., concurring)).

[32] As the Supreme Court remarked in *United States v. United States District Court*:

> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

407 U.S. 297, 314 (1972).

[33] *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 6-7 (2000) ("Whatever the surveillance technique, domestic security surveillance may also chill the free expression protected by the First Amendment.").

[34] 407 U.S. at 314.

[35] 18 U.S.C. §§ 2510-2522 (1994 & Supp. V 1999).

[36] 50 U.S.C. §§ 1801-1811 (1994 & Supp. V 1999).

sive surveillance authority in a wide range of circumstances. And yet, proponents of the USA PATRIOT Act pushed for the swift passage of this controversial piece of legislation—claiming that expanded governmental surveillance authority would be an essential weapon in combating the immediate threat of terrorism[37]—without first inquiring into how the Act would disrupt the delicate balance struck with Title III and FISA. Only with a thorough understanding of the precursors to, purposes of, authority granted by, and protections afforded under Title III and FISA can one begin to understand the far-reaching and unwarranted surveillance authority bestowed upon law enforcement and intelligence agencies by the USA PATRIOT Act.

A. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*

Title III was the legislative response to the Supreme Court's landmark decision in *Katz v. United States,* where the Court, influenced by notions of privacy, established that governmental interception of an individual's telephone conversation, conducted without the target's consent, constitutes a search and seizure within the meaning of the Fourth Amendment.[38] Although the *Katz* decision definitively barred warrantless governmental surveillance in the context of criminal investigations, in a highly controversial footnote the Court left the door open for warrantless surveillance in circumstances concerning national security.[39] In a concurring opinion, Justice White indicated that the Supreme Court should not require the President to obtain a warrant for national security matters where the President had determined the reasonableness of the surveillance.[40] Troubled by Justice White's statement, Justice Douglas, joined by Justice Brennan, responded:

> Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be . . . . The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases . . . . Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers . . . I cannot agree that where spies and saboteurs are

---

[37] *See* Clymer, *supra* note 6, at A1 ("'The president is pleased that Congress has acted quickly to provide additional tools in fighting the war on terrorism . . . .'" (quoting Claire Buchan, Deputy Press Secretary to the President).

[38] 389 U.S. 347, 353 (1967).

[39] "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Id.* at 358 n.23.

[40] *Id.* at 364 (White, J., concurring).

> involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.[41]

Although the Court would not address the executive branch's authority in approving intelligence surveillance for another five years, this early dialogue presented a preview to the forthcoming debate concerning this greatly contested matter.

Responding to the majority holding of *Katz*, Congress enacted Title III as a means to implement a uniform procedure for conducting constitutionally acceptable electronic surveillance. Title III authorizes law enforcement agents to engage in surveillance activities for criminal investigative purposes upon a judge's finding of probable cause that a serious crime[42] has been or is about to be committed, and an award of a warrant[43]—in compliance with the Fourth Amendment's directive. Generally, all criminal surveillance must be authorized by a judge of competent jurisdiction.[44] In an emergency situation,[45] however, where there is immediate danger of death or serious injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime,[46] law enforcement may engage in warrantless wiretapping, so long as an application for a warrant is made within forty-eight hours of the commencement of interception.[47]

The congressional findings accompanying Title III clearly illustrate Congress's dual intent in creating this extensive piece of legislation: "to promote more effective control of crime while protecting the privacy of individual thought and expression."[48] The findings indicate that:

> (c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communica-

---

[41] *Id.* at 359-60 (Douglas, J., concurring, joined by Brennan, J.).

[42] 18 U.S.C. § 2516(1) (1994 & Supp. V 1999) (enumerating the types of offenses for which a wiretap may be granted).

[43] 18 U.S.C. § 2518(3)(a) (1994).

[44] 18 U.S.C. § 2518(1) (1994); *see also* 18 U.S.C. § 2516 (1994 & Supp. V 1999).

[45] An emergency must be reasonably determined as such "by any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State." 18 U.S.C. § 2518(7) (1994).

[46] 18 U.S.C. § 2518(7)(a)(iii) (1994).

[47] 18 U.S.C. § 2518(7) (1994).

[48] United States v. United States Dist. Court, 407 U.S. 297, 302 (1972).

> tions to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.
>
> (d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court . . . .[49]

The probable cause requirement of Title III is integral to the protection of individual privacy from the invasive nature of wiretaps and is a particularly important concept to appreciate in comparing Title III and FISA since FISA does not require that this protective element be demonstrated to the court before surveillance authority is granted. Meeting the probable cause requirement of Title III is a substantial threshold that the applicant for wiretap authority must reach to the satisfaction of the reviewing judge before such intrusive authority will be permitted.[50] To protect against unreasonable searches and seizures as provided by the Fourth Amendment, Title III explicitly requires that the judge ascertain the existence of probable cause "that an individual is committing, has committed, or is about to commit a particular offense"[51] before granting wiretap authority. In *United States District Court*, the Supreme Court elaborated on the importance of the probable cause requirement in stating that it is the "very heart of the Fourth Amendment directive: that, where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private . . . conversation."[52]

Although Title III is broad in scope, it is clear that the statute was not meant to infringe upon the Executive's long-standing surveillance authority over matters concerning foreign intelligence. As the D.C. Circuit noted in *Chagnon v. Bell*, "every President since Franklin D. Roosevelt has claimed the 'inherent' constitutional power to authorize warrantless surveillance in cases vitally affecting the national security. Furthermore, all presidents to hold office since *Katz* was decided have

---

[49] Act of June 19, 1968, Pub. L. No. 90-351, tit. III, § 801, 82 Stat. 211.

[50] In an application for wiretap authority, the applicant must provide the court with information, beyond that needed to establish probable cause, that a crime has been or is soon to be committed. The information necessary for a wiretap application is detailed in 18 U.S.C. § 2518 (1994 & Supp. V 1999).

[51] 18 U.S.C. § 2518(3)(a) (1994).

[52] 407 U.S. at 316.

advocated a broad exception to the warrant requirement for surveillance targeted at agents of foreign governments."[53] The original version of Title III unequivocally stated:

> 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. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.[54]

This initial provision was repealed in 1978, the year FISA was enacted, and replaced by § 2511(2)(e) and (f), which similarly indicates in pertinent part that "[n]othing contained in this chapter . . . shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications."[55]

B. *The Foreign Intelligence Surveillance Act of 1978*

1. The History Behind FISA

The Foreign Intelligence Surveillance Act has a less straightforward history than Title III. A handful of influential cases addressing the Executive's power to authorize intelligence surveillance, along with congressional findings of the executive branch's widespread abuse of surveillance power authorized for "intelligence purposes," motivated FISA's promulgation. The first case to bring national attention to the Executive's intelligence surveillance authority was *United States District Court*, in which the Attorney General authorized warrantless electronic surveillance of the defendant, a United States citizen

---

[53] 642 F.2d 1248, 1259-60 (D.C. Cir. 1980).

[54] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 2511(3), 82 Stat. 197, 214 (repealed 1978).

[55] 18 U.S.C. § 2511(2)(f) (1994).

suspected of conspiring to destroy government property.[56] The Attorney General, in his affidavit to the district court, alleged that the wiretap of the defendant was employed "'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.'"[57] By recognizing § 2511(3) of Title III as leaving the Executive's authority undisturbed "to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government," the Court distinguished the power of the executive branch to conduct surveillance for intelligence purposes from the function of Title III as setting forth procedures authorizing surveillance activities in criminal investigations.[58] Although the Court acknowledged the Executive's intelligence-gathering authority, it held that the Fourth Amendment does not permit warrantless wiretaps in cases involving *domestic* threats to national security.[59] The Court was clear in limiting the scope of its decision to the surveillance of domestic organizations and thus did not address whether wiretaps authorized solely by the Executive would be an acceptable means of gathering intelligence information pertaining to a foreign power or agent of a foreign power.[60]

Unfettered by judicially imposed constraints on the Executive's power to authorize surveillance for foreign intelligence investigations, in the years following *United States District Court* the Executive tested the boundaries of his statutory authority—a practice which resulted in several cases that proved significant in the formation of FISA. Of the five federal courts of appeals that addressed this controversial subject, four readily accepted the surveillance power of the Executive, while the D.C. Circuit refused to follow suit. In determining the legality of the warrantless wiretaps authorized and employed in each of the following cases, the courts generally focused on whether the *primary purpose* of the wiretap was to gather foreign intelligence information. If the primary purpose standard was met, the surveillance was by and large found to be acceptable.

---

[56] 407 U.S. at 299. Although this case arose from a criminal proceeding in which the United States charged three defendants with conspiracy to destroy government property, the appeal dealt primarily with one defendant who was charged with the dynamite bombing of a Central Intelligence Agency office in Ann Arbor, Michigan. *Id.*

[57] *Id.* at 300 (quoting Affidavit of Attorney General John N. Mitchell).

[58] *Id.* at 310.

[59] *Id.* at 320-21.

[60] *Id.* at 308.

In *United States v. Brown*, several conversations of the appellant, a U.S. citizen, were intercepted through the government's electronic surveillance of other targets, as authorized by the Attorney General.[61] The Fifth Circuit affirmed the lower court's finding that the wiretaps of the third party targets were conducted for the sole purpose of gathering foreign intelligence and therefore were legal.[62] In supporting the validity of the Executive's surveillance authority, the court stated, "because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, we reaffirm . . . that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence."[63]

In *United States v. Butenko*, a Soviet national and an American citizen appealed their convictions for transmitting to a foreign government materials and information relating to the national defense.[64] The Third Circuit accepted the lower court's decision that the surveillance was within the power of the Executive, as it was primarily designed to determine the leak of sensitive information concerning foreign policy and military posture.[65] The court endorsed the foreign intelligence warrant exception by stating, "While we acknowledge that requiring prior approval of electronic surveillance . . . might have some salutary effects . . . the better course is to rely . . . on the good faith of the Executive . . . . [A] strong public interest exists: the efficient operation of the Executive's foreign policy-making apparatus depends on a continuous flow of information."[66] The Ninth Circuit in *United States v. Buck*, simply cited to *Butenko* when it acknowledged that "[f]oreign security wiretaps are a recognized exception to the general warrant requirement."[67]

Finally, in *United States v. Troung Dinh Hung*,[68] the Attorney General authorized a massive surveillance[69] of Truong, a Vietnamese citi-

---

[61] 484 F.2d 418, 421 (5th Cir. 1973).

[62] *Id.* at 426-27.

[63] *Id.* at 426.

[64] 494 F.2d 593, 596-97 (3d Cir. 1974).

[65] *Id.* at 608.

[66] *Id.* at 605.

[67] 548 F.2d 871, 875 (9th Cir. 1977).

[68] 629 F.2d 908 (4th Cir. 1980). Although this case was decided in 1980, the surveillance in question was authorized in 1977, before the enactment of FISA. *Id.* at 912.

[69] "Truong's phone was tapped and his apartment was bugged from May 1977 to January 1978. The telephone interception continued for 268 days and every conversation, with possibly one exception, was monitored and virtually all were taped. The

zen who was known to be passing diplomatic cables and other classified papers of the United States government's dealings with Southeast Asia to North Vietnamese government officials. In affirming the district court's finding that the executive branch need not always obtain a warrant for foreign intelligence surveillance, the Fourth Circuit found that "the executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons . . . . We . . . reject the government's assertion that, if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment."[70]

In *Zweibon v. Mitchell*, the D.C. Circuit was the sole federal court of appeal to find the Executive's warrantless foreign intelligence surveillance authority to be impermissible.[71] Here, the appellants were members of the Jewish Defense League (JDL)[72] who brought an action against Attorney General John Mitchell and agents of the FBI for conducting illegal electronic surveillance.[73] Although the Attorney General claimed that the surveillance of the JDL was "essential to protect this nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States,"[74] the court determined that the true and primary purpose of the extensive surveillance was to provide the government with advance information concerning JDL activities which "could create a situation of international embarrassment to this country."[75] Upon this conclusion, and following an exhaustive review of the

---

eavesdropping device was operative for approximately 255 days and it ran continuously." *Id.* at 912.

[70] *Id.* at 915.

[71] 516 F.2d 594, 659 (D.C. Cir. 1975) ("We have held that the electronic surveillances involved in this case were illegal because they were executed without a warrant.").

[72] At the time, the JDL vocally opposed the Soviet government's restrictive emigration policies relating to Jews within the Soviet Union and engaged in a variety of activities ranging from peaceful demonstrations to acts of violence to further their goals and demonstrate their political beliefs. *Id.* at 608.

[73] The telephones of the appellants were wiretapped during the month of October 1970 and from January 5 through June 30, 1971. *Id.* at 605. Furthermore, "the Government prosecutor admitted that six telephone lines had been involved in the taps and that there were 'volumes and volumes' of transcripts of intercepted communications." *Id.* at 606. During the period that the wiretaps were installed, neither the Attorney General nor other officials from his office reviewed the information on the tapes or evaluated the necessity for continuation of the surveillance. *Id.* at 610.

[74] *Id.* at 607.

[75] *Id.* at 609 n.24.

historical policy of executive-authorized surveillance[76] and prior case law, the court announced a holding very similar to that of *United States District Court*—that a "warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power, even if the surveillance is installed under presidential directive in the name of foreign intelligence gathering for protection of the national security."[77] In dictum, the court discussed the earlier cases of *Brown* and *Butenko*, finding these courts' analyses wholly inadequate as they simply converted the Executive's need to gather intelligence information into an absolute right to conduct warrantless surveillance—without giving sufficient thought to First and Fourth Amendment interests that may be infringed upon by allowing the Executive to bypass judicial scrutiny.[78] The court suggested that the proper analysis would ascertain whether requiring the Executive to obtain a warrant before engaging in intelligence activities would frustrate the acquisition of such information.[79] In determining that the warrant procedure would not unduly impede the intelligence gathering function of the Executive, the court analyzed five possible reasons for exempting the Executive's intelligence activities from the warrant requirement, finding none sufficiently persuasive to justify a warrant exception: (1) the lack of judicial competence in matters of intelligence surveillance, (2) the danger of security leaks, (3) the threat of "strategic" information-gathering—the fact that surveillance tends to be authorized for intelligence purposes rather than for gathering information of criminal activity, (4) the possibility that delay would hinder the success of surveillance, and (5) the administrative burden on the courts and executive branch.[80] Based upon a review of these factors, the plurality opinion expressed the view that "absent exigent circumstances, *all* warrantless electronic surveillance is unreasonable and therefore unconstitutional."[81]

In addition to Congress's intent to resolve the disagreement be-

---

[76] Although the court recognized the long history of executive-authorized surveillance in situations concerning national security, the court made clear that "this practice has never received Supreme Court approval, and there can be no doubt that an unconstitutional practice, no matter how inveterate, cannot be condoned by the judiciary." *Id.* at 616.

[77] *Id.* at 614.

[78] *Id.* at 639-41.

[79] *Id.* at 640.

[80] *See id.* at 641-52 (discussing in detail how the listed factors are insufficient to exempt the Executive's intelligence gathering activities from the warrant requirement).

[81] *Id.* at 614 (emphasis added).

tween the circuits as to the power of the Executive in authorizing intelligence surveillance, Congress was further encouraged to clarify and curtail the intelligence-gathering functions of the Executive once it was made aware of the executive branch's long-standing and pervasive abuse of this power. In the early 1970s, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee") conducted an investigation of the United States intelligence agencies to determine the extent of alleged invasions of individual privacy interests.[82] The Committee uncovered the alarming truth that the CIA spied illegally on as many as seven thousand Americans through the 1960s and early 1970s in Operation CHAOS, including individuals involved in the peace movement, student activists, and black nationalists.[83] The Church Committee Report[84] revealed how the absence of clear statutory or judicial standards led to widespread warrantless electronic surveillance of individuals who were not associated in any way with a foreign power, did not seem to pose a threat to national security, and were not suspected of being involved in criminal activity.[85] These findings compelled Congress to create a statutory code to definitively determine the role of the Executive in authorizing intelligence surveillance of foreign powers and individuals engaged in activities deemed to threaten national security. In 1978, FISA was enacted into law.[86]

2. FISA Deconstructed

FISA provides statutory authorization for electronic surveillance in the limited context when surveillance is sought to target a foreign

---

[82] Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 806-07 (1989) (noting the activities of the Church Committee in investigating intelligence agencies and finding that "warrantless electronic surveillance had been used against United States Citizens who were not readily identifiable as reasonable sources of foreign intelligence information").

[83] "Operation CHAOS involved an extensive program of information sharing from the FBI and other agencies to the CIA. CIA received all of the FBI's reports on the American peace movement, which numbered over [one thousand per month] by June of 1970, according to [the] . . . 'Church Committee Report.'" ACLU, *Surveillance of Americans: How the Senate Anti-Terrorism Bill Puts the CIA Back in the Business of Spying on Americans*, *at* http://www.aclu.org/congress/1100901b.html (Oct. 9, 2001).

[84] 2 SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, FINAL REPORT, S. REP. NO. 94-755 (2d Sess. 1976).

[85] Cinquegrana, *supra* note 82, at 806-07.

[86] Pub. L. No. 95-511, § 301, 92 Stat. 1783, 1798 (1978).

power or an agent of a foreign power,[87] and when the purpose of the surveillance is to obtain foreign intelligence information.[88] By enacting FISA, "Congress sought to accommodate and advance both the government's interest in pursuing legitimate intelligence activity and the individual's interest in freedom from improper government intrusion."[89] FISA broadly defines the term "foreign power" as a foreign government, a faction of a foreign nation, a group engaged in international terrorism, an entity directed and controlled by a foreign government, or a foreign-based political organization not substantially composed of United States persons.[90] An "agent of a foreign power" is defined as any non-United States person who: acts in the United States as an officer, employee, or member of a foreign power; or acts on behalf of a foreign power engaging in clandestine intelligence activities in the United States.[91] The definition of "agent of foreign power" also includes any persons: who knowingly perform clandestine

---

[87] 50 U.S.C. § 1804(a)(4)(A) (1994). *See generally* United States v. Cavanagh, 807 F.2d 787, 788-89 (9th Cir. 1987) (outlining FISA's requirements for electronic surveillance of foreign powers and their agents).

[88] 50 U.S.C. § 1804(a)(7)(B) (1994). The Act defines "foreign intelligence information" as:

> information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

50 U.S.C. § 1801(e)(1) (1994).

[89] *Cavanagh*, 807 F.2d at 789; *see also* ACLU v. Barr, 952 F.2d 457, 461 (D.C. Cir. 1991) ("By enacting FISA, Congress sought to resolve doubts about the constitutionality of warrantless, foreign security surveillance and yet protect the interests of the United States in obtaining vital intelligence about foreign powers."); United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988) ("Congress enacted FISA in 1978 'to establish procedures for the use of electronic surveillance in gathering foreign intelligence information.'" (quoting *In re* Kevork, 788 F.2d 566, 569 (9th Cir. 1986))); United States v. Pelton, 835 F.2d 1067, 1074 (4th Cir. 1987) ("FISA was passed by Congress in 1978 to create a '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.'" (quoting S. REP. NO. 95-604, at 15, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916)).

[90] 50 U.S.C. § 1801(a) (1994); *see also* United States v. Badia, 827 F.2d 1458, 1462 (11th Cir. 1987) ("FISA contains several definitions of 'foreign power' and 'agent of a foreign power' pertinent to this case. 'Foreign power' includes 'a group engaged in international terrorism or activities in preparation therefore.'" (quoting 50 U.S.C. § 1801(a)(4) (1994))).

[91] 50 U.S.C. § 1801(b)(1) (1994).

intelligence gathering activities on behalf of a foreign power, whose activities involve or may involve a violation of the criminal statutes of the United States; who knowingly engage in sabotage or international terrorism on behalf of a foreign power; who knowingly enter the United States under a false identity for a foreign power; or who knowingly aid, abet, or conspire with any person in the conduct of the above activities.[92] Furthermore, "United States person" is defined as a citizen of the United States or an alien lawfully admitted for permanent residence.[93]

Each application for surveillance authorization must be made by a federal officer, with the approval of the Attorney General, to the Foreign Intelligence Surveillance Court (FISC).[94] FISA mandates the formation of this special court, which consists of seven district court judges appointed by the Chief Justice of the United States, to hear all FISA applications for electronic surveillance.[95] A FISC judge is permitted to authorize a FISA surveillance if she finds, among other factors,[96] that

> there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment.[97]

While it is integral to the surveillance authorization process that the FISC judge make this finding, the court in *United States v. Duggan* clarified the role of the FISC by stating that once the Attorney General certifies the application of a federal officer, the surveillance request is "subjected to only minimal scrutiny by the courts."[98]

Proceedings of the FISC, including applications made and orders

---

[92] *Id.* § 1801(b)(2) (1994 & Supp. V 1999).

[93] *Id.* § 1801(i) (1994).

[94] *Id.* § 1804(a); *see also Barr*, 952 F.2d at 461 ("Before an application seeking authorization for surveillance may be filed with the FISA Court, the Attorney General must personally approve it.").

[95] 50 U.S.C. § 1803 (1994); *see also* United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) ("The special FISA court is composed of seven United States District Judges designated by the Chief Justice of the United States." (citing 50 U.S.C. § 1803(a) (1982))).

[96] 50 U.S.C. § 1805(a)(1)-(5) (1994).

[97] *Id.* § 1805(a)(3)(A); *see Barr*, 952 F.2d at 461-62 (discussing the factors a FISA judge must establish before she is authorized to enter an order approving surveillance pursuant to § 1805); United States v. Badia, 827 F.2d 1458, 1463 (11th Cir. 1987) (same); *Cavanagh*, 807 F.2d at 789 (same).

[98] 743 F.2d 59, 77 (2d Cir. 1984).

granted, are conducted and maintained in secrecy due to national security concerns regarding the information submitted to the court.[99] Although such secrecy may be justified—as public knowledge of applications and granted surveillance authority likely would undermine the success of the information gathering process—the secret nature of these proceedings is troublesome, particularly to the targets who later wish to determine the validity of a surveillance application or grant of authority. In *United States v. Badia*, the target of FISA surveillance sought disclosure of the FISA application to review it for errors or falsehoods, as he believed that the surveillance was imposed not to seek foreign intelligence information, but rather to conduct a criminal investigation.[100] The Eleventh Circuit denied the request, stating that "where the Attorney General files an 'affidavit under oath, that disclosure or an adversary hearing would harm the national security of the United States,' § 1806(b) of FISA provides for *in camera, ex parte* review of the application by the court."[101] Therefore, although the highly confidential nature of investigating targets suspected of engaging in activities that may undermine national security clearly warrants greater precautions,[102] this rationale is little consolation to innocent parties who have limited means to discover the reason for a complete violation of their privacy. As the Supreme Court recognized in *Mitchell v. Forsyth*, "[n]ational security tasks . . . are carried out in secret; open conflict and overt winners and losers are rare. Under such circumstances, it is far more likely that actual abuses will go uncovered than that fancied abuses will give rise to unfounded and burdensome litigation."[103]

Title III diverges from FISA in a very important respect, as it provides for the disclosure of Title III applications made and orders granted upon a showing of good cause by the target.[104] Additionally, Title III includes a notice requirement, providing that within a reasonable time after either the denial of an application or the termination of surveillance, the issuing or denying judge will serve both the target and third parties to intercepted communications notice of the

---

[99] 50 U.S.C. § 1803(c) (1994).

[100] 827 F.2d at 1462.

[101] *Id.* at 1464 (quoting 50 U.S.C. § 1806(b) (1994)).

[102] *See generally* Gregory E. Birkenstock, Note, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 845 (1992) ("Even under FISA's regulatory scheme, the words 'national security' appear to have acquired a near-talismanic significance for many courts.").

[103] 472 U.S. 511, 522 (1985).

[104] 18 U.S.C. § 2518(8)(b) (1994).

application or order, information concerning the period of surveillance, and whether or not communications were intercepted.[105] This protective measure allows the target of intercepted communications an opportunity to bring suit if she believes that the authorized surveillance violated her Fourth Amendment rights. FISA does not provide a similar privacy protection to targets of a completed FISA surveillance. This practically ensures that intrusive wiretaps that do not uncover incriminating information, and therefore do not result in prosecutions, never will be made known to the target.

Each federal officer seeking surveillance authority must satisfy the numerous application criteria explicitly laid out in § 1804 of FISA, including but not limited to: the identity or a description of the target, the facts or circumstances leading the applicant to believe that the target is a foreign power or an agent of a foreign power, that each of the sites of surveillance is being used or is about to be used by a foreign power or an agent of a foreign power, a statement of the proposed minimization procedures, a detailed description of the nature of the information sought, that a certifying official deems that the information sought is foreign intelligence information, that such information cannot reasonably be obtained by normal investigative techniques, and that the purpose of the surveillance is to obtain foreign intelligence information.[106] Although these extensive requirements suggest that the applying federal officer must have engaged in a thorough investigation of the target to supply the court sufficient information, none of the criteria necessary for application of FISA surveillance court orders rise to the level of the Fourth Amendment's probable cause requirement. The federal officer does not need to demonstrate that a criminal or unlawful act has been or is about to be committed before she is granted authority to intrude upon the privacy interests of the specified target.[107] Theoretically, the officer is not seeking evidence of criminal activities on which to base a prosecution, but rather is seeking information regarding foreign intelligence activities that may compromise national security.

---

[105] *Id.* § 2518(8)(d) (1994).

[106] 50 U.S.C. § 1804(a)-(b) (1994); *see also* ACLU v. Barr, 952 F.2d 457, 461 (D.C. Cir. 1991) (setting out the facts that an application to the FISC for a surveillance court order must include); United States v. Badia, 827 F.2d 1458, 1463 (11th Cir. 1987) (same); United States v. Cavanagh, 807 F.2d 787, 789 (7th Cir. 1987) (same).

[107] If a given target is a United States person, the most a federal officer will need to demonstrate to the FISC is that the target's activities "involve or *may involve* a violation of the criminal statutes of the United States"—a low threshold of proof to obtain surveillance authorization. 50 U.S.C. § 1801(b)(2)(A) (1994) (emphasis added).

Despite the comprehensive requirements of § 1804, many libertarians are concerned that in practice, a "FISA interception order requires little beyond probable cause to believe that the person or group targeted is an agent of a foreign power or an international terrorist group."[108] Additionally, upon reviewing the statistics regarding grants of surveillance authority by the FISC, it becomes increasingly clear that the court's actual standards may not be too exacting. For example, "[a]ccording to the Center for Democracy and Technology, the special court, which approved more than 1,000 surveillance requests last year, has denied only one request in 22 years."[109]

Beyond FISA's seemingly lenient warrant requirements, FISA further empowers the Executive to authorize electronic surveillance as a means to acquire foreign intelligence information for periods of up to one year. Authorization under FISA is appropriate where the Attorney General certifies that the acquired communications are exclusively between foreign powers or are made by individuals under the exclusive control of a foreign power, and that there is no substantial likelihood that the surveillance will acquire communication to which a United States person is a party.[110] Although the Attorney General must transmit to the FISC a copy of his certification,[111] this document remains sealed unless an application for a court order is made, or the certification is later necessary to determine the legality of the surveillance.[112] Therefore, the FISC never reviews the Attorney General's actions unless an aggrieved party brings suit. This unfettered authority of the Executive is problematic in that the Attorney General is not a neutral party in matters of foreign intelligence,[113] and may not have the same ability as an impartial judge to ensure that the requirements of § 1802 are sufficiently met. Without judicial oversight, the Attorney General's surveillance powers remain largely unchecked, and abuses could occur. As the Supreme Court explained in *United States District Court*, "[t]he independent check upon executive discretion is not sat-

---

[108] Ronald L. Kuby, *Ashcroft Should Slow Down His Rush to Change Our Laws*, NEWSDAY (New York), Oct. 4, 2001, at A44.

[109] Marcia Coyle, *Sharp Debate on Surveillance Law: Pick Between Two Little Words Makes a Big Difference*, NAT'L L.J., Oct. 8, 2001, at A13.

[110] 50 U.S.C. § 1802(a)(1) (1994).

[111] *Id.* § 1802(a)(3) (1994).

[112] *Id.*

[113] *See supra* text accompanying note 41 (providing Justice Douglas's opinion that "[i]n matters where [the President or Attorney General] believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be").

isfied . . . by 'extremely limited' post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances that failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights."[114]

The Attorney General also may authorize warrantless surveillance activities upon reasonably determining that an emergency situation requires immediate acquisition of foreign intelligence information.[115] Under these circumstances, the Attorney General must make an application to a FISC judge within twenty-four hours after the surveillance is authorized.[116] This raises yet another concern; namely, that in practice the Attorney General may designate any situation an "emergency," as the statute does not define what elements must be present for a set of circumstances to be deemed as such. Although the Attorney General must notify the court within a twenty-four hour period of its activities, once the surveillance has commenced it is unlikely the court will interfere.

3. FISA in Practice

The first courts to address this new statute unanimously held FISA to be constitutional and sufficient in protecting the Fourth Amendment rights of the individuals subject to its authorized surveillance. In *Duggan*, the FBI obtained a court order to conduct surveillance on four individuals[117] working on behalf of the Provisional Irish Republican Army to acquire weapons in the United States for export to Northern Ireland for use in terrorist activities.[118] Here, the Second Circuit found "the procedures fashioned in FISA [to be] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information."[119] In *United States v. Cavanagh*, government officers intercepted a telephone conversation of the appellant, an American citizen, pursuant to FISA authorization, in which he offered to sell

---

[114] United States v. United States Dist. Court, 407 U.S. 297, 317-18 (1972).

[115] 50 U.S.C.A. § 1805(f) (West Supp. 2001).

[116] *Id.*

[117] The four defendants included an Irish national who sought political asylum in the United States, an American citizen, and two aliens living illegally in the United States. United States v. Duggan, 743 F.2d 59, 65 (2d Cir. 1984).

[118] *See id.* at 64-65 (upholding convictions based on electronic surveillance authorized under FISA).

[119] *Id.* at 73.

defense secrets to representatives of the Soviet Union.[120] The Ninth Circuit made clear that "FISA satisfies the constraints the Fourth Amendment places on foreign intelligence surveillance conducted by the government."[121] Additionally, upon reviewing a court-ordered FISA surveillance of a former National Security Agency (NSA) employee suspected of selling classified information about NSA programs to the Soviet Union, the Fourth Circuit in *United States v. Pelton* affirmed the district court's finding that the primary purpose of the surveillance was to gather foreign intelligence information.[122] The court stated that "[w]e now join the other courts of appeal that have reviewed FISA and held that the statute meets constitutional requirements. FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment within the context of foreign intelligence activities."[123] Additionally, in *Badia*, as discussed above, while the Eleventh Circuit did not explicitly make reference to the constitutionality of FISA, the court clearly analyzed the surveillance target's claims under FISA,[124] thereby implicitly accepting the statute as passing constitutional scrutiny.

Although the courts that have addressed FISA universally have found the statutory provisions constitutional,[125] a few pre-FISA courts acknowledged the potential for abuse that could result from permitting a foreign intelligence exception to the FISA warrant requirement. In *Chagnon v. Bell*, the D.C. Circuit warned that "when the foreign agent exception is invoked to justify warrantless surveillance, courts must be alert to the possible pretextuality of the claim."[126] Therefore, the court must determine whether there exists a "'direct link between the wiretap target and a foreign interest as a justification for surveil-

---

[120] *See* 807 F.2d 787, 788 (9th Cir. 1987) (affirming the district court's refusal to suppress the "fruits" of the electronic surveillance).

[121] *See id.* at 790 (citing *Duggan*, 743 F.2d at 72-74; *In re* Kevork, 634 F. Supp. 1002, 1010-14 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986); United States v. Megahey, 553 F. Supp. 1180, 1185-92 (E.D.N.Y. 1982); United States v. Falvey, 540 F. Supp. 1306, 1311-14 (E.D.N.Y. 1982)).

[122] 835 F.2d 1067, 1076 (4th Cir. 1987) ("The FISA evidence in this case was obtained in accordance with the requirements of the statute, and was properly admitted by the district court.").

[123] *Id.* at 1075 (citing *Cavanagh*, 807 F.2d at 792; *Duggan*, 743 F.2d at 76).

[124] United States v. Badia, 827 F.2d 1458, 1462-65 (11th Cir. 1987).

[125] *See Pelton*, 835 F.2d at 1075 ("We now join the other courts of appeal that have reviewed FISA and held that the statute meets constitutional requirements."); *Cavanagh*, 807 F.2d at 790 ("We find that the probable cause showing required by FISA is reasonable.").

[126] 642 F.2d 1248, 1260 (D.C. Cir. 1980).

lance' and . . . [whether] the surveillance was 'reasonably intended to guard national security data from foreign intelligence agencies.'"[127] Moreover, in *United States v. Truong Dinh Hung*, after approving the warrantless FISA surveillance of a target suspected of passing classified United States documents to the North Vietnamese government, the Fourth Circuit cautioned,

> [B]ecause individual privacy interests are severely compromised any time the government conducts surveillance without prior judicial approval, this foreign intelligence exception to the Fourth Amendment warrant requirement must be carefully limited to those situations in which the interests of the executive are paramount. First, the government should be relieved of seeking a warrant *only* when the object of . . . the surveillance is a foreign power, its agent or collaborators . . . . Second, . . . the executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons.[128]

While both of these cases were decided applying pre-FISA law,[129] their cautionary statements remain appropriate in light of the warrantless surveillance authority granted to the Executive through §§ 1802[130] and 1805(f)[131] of FISA.

III. SURVEILLANCE LAW UNDER THE USA PATRIOT ACT

A. *"The Purpose" of Surveillance Becomes "A Significant Purpose"—Permitting Primarily Criminal Investigations to Fall Within FISA Surveillance Authority*

Section 218 of the USA PATRIOT Act amends FISA § 1804(a)(7)(B). Now, in an application to the FISC, a federal officer no longer has to demonstrate that "*the purpose* of the surveillance is to obtain foreign intelligence information,"[132] but may obtain surveillance authorization under the less stringent showing that "*a significant purpose* of the surveillance is to obtain foreign intelligence information."[133] This slight alteration in the language of § 1804 is highly sig-

---

[127] *Id.* (quoting Halperin v. Kissinger, 606 F.2d 1192, 1204 (D.C. Cir. 1979)).

[128] 629 F.2d 908, 915 (4th Cir. 1980) (emphasis added).

[129] The courts used pre-FISA law because the wiretaps in question were authorized before 1978, the year FISA was enacted.

[130] *See* 50 U.S.C.A. § 1802 (West Supp. 2001) (permitting electronic surveillance authorization without a court order).

[131] *See id.* § 1805(f) (West Supp. 2001) (permitting warrantless electronic surveillance authorization in emergency situations).

[132] 50 U.S.C. § 1804(a)(7)(B) (1994) (emphasis added).

[133] H.R. Res. 3162, 107th Cong. § 218 (2001) (enacted) (emphasis added).

nificant in that it is extremely likely to increase the types of court-ordered investigations that are carried out in the name of "foreign intelligence investigations" under FISA. Considering the fact that the FISC has only turned down one surveillance application since its inception,[134] it becomes even more likely that the court will authorize all forthcoming applications under this more lenient standard.

The concern raised by this amendment is that under the new broadened scope of § 1804, both intelligence *and* law enforcement agents will bring applications for electronic surveillance to the FISC when the primary purpose of the surveillance is an investigation of criminal activities. Thus, the amended FISA will be used as a means to undertake surveillance without demonstrating the heightened standard of probable cause required under Title III for criminal wiretaps. This potential end-run around the Fourth Amendment's probable cause requirement for criminal investigations contradicts the rationale for permitting a lower threshold for obtaining FISA wiretaps. No longer will this lesser standard solely authorize investigations of primarily foreign intelligence activities where the rights of Americans are generally not implicated. Instead, FISA will be employed to approve investigations of predominantly criminal activities, including purely domestic criminal acts—in explicit violation of the Fourth Amendment.[135] Now, under section 218 a criminal investigation can be the primary purpose of a FISA investigation, with foreign intelligence information as a secondary, albeit "significant purpose."[136] Senator

---

[134] *See* Coyle, *supra* note 109, at A13 ("According to the Center for Democracy and Technology, the special court, which approved more than 1,000 surveillance requests last year, has denied only one request in 22 years.").

[135] *See* 147 CONG. REC. S10,593 (daily ed. Oct. 12, 2001) (statement of Sen. Cantwell) ("Where information is sought for the purpose of law enforcement, we must ensure that fourth amendment protections apply. Much of the fear about the legislation is based on legitimate concern that information gathered ostensibly for intelligence and defense purposes could be used for law enforcement purposes."). Senator Cantwell went on to make a distinction between intelligence and law enforcement uses of surveillance. She argued that "[t]he intelligence community does not prosecute and lock up its targets; it uses information to intervene against foreign nationals seeking to harm America." *Id.* In comparison, Cantwell argued that the "law enforcement community has a different mission, to catch and prosecute criminals in our courts of law. Because law enforcement acts upon U.S. citizens, it must do so within the bounds of the Constitution." *Id.*

[136] H.R. Res. 3162, 107th Cong. § 218 (2001) (enacted); *see* 147 CONG. REC. S10,593 (daily ed. Oct. 12, 2001) (statement of Sen. Cantwell) ("[T]he possibility remains that the primary purpose of the wiretap would be a criminal investigation, without the safeguards of the title III wiretap law and the protections under the fourth amendment that those fulfill.").

Leahy recognized that by amending the language of FISA, "the USA Act[137] would make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution."[138] The Senator further acknowledged that "[t]his is a disturbing and dangerous change in the law."[139]

Furthermore, as the USA PATRIOT Act's amendment to FISA does not provide a definition of "significant purpose," it is unclear how far the FISC will stretch its interpretation of this phrase to accommodate law enforcement and intelligence agencies in their quest to increase surveillance as a response to the September 11th terrorist attacks. Yet, the consequences of this amendment to FISA go far beyond investigations of the September 11th tragedy. Now, surveillance authority for investigations seeking information primarily pertaining to purely domestic criminal activities may be granted under FISA with no showing of probable cause that a serious crime has been or will soon be committed.

Several courts have addressed the situation in which a surveillance target contends that the actual purpose of the surveillance was criminal investigation as opposed to the government's purported rationale of foreign intelligence gathering. Pre-FISA, circuit courts addressing this issue made clear that they would only uphold executive authorization through post-surveillance judicial review when conducted for the "primary purpose" of gathering foreign intelligence information.[140] Although these cases involve situations where the Executive engaged in warrantless surveillance, the accounts of these courts apply equally to a discussion concerning the standard for court-ordered surveillance under FISA. In *Butenko*, the Third Circuit expressly admonished that "[s]ince the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental."[141] The Fifth Circuit also made clear its position on the use of FISA-authorized surveillance for the purpose of engaging in criminal investigations in *Brown*, by asserting "[t]here is no indication that de-

---

[137] At the time of this statement, the Senate was discussing the Senate's precursor to the USA PATRIOT Act, yet the provision is identical to the one enacted into law.

[138] 147 CONG. REC. S10,593 (daily ed. Oct. 12, 2001) (statement of Sen. Leahy).

[139] *Id.*

[140] *See supra* notes 61-70 and accompanying text (discussing cases).

[141] United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974).

fendant's telephone conversations were monitored for the purpose of gaining information to use at his trial, a practice we would immediately proscribe with appropriate remedy."[142] The Fourth Circuit in *Truong* similarly found:

> [T]he executive should be excused from securing a warrant only when the surveillance is conducted "primarily" for foreign intelligence reasons .... [O]nce surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution. We thus reject the government's assertion that, if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment.[143]

These statements plainly reveal these courts' belief that anything less than an indication that the primary purpose of a given surveillance is to gather foreign intelligence information would be unacceptable. Furthermore, post-FISA, the Second Circuit in *Duggan* stated that "[t]he requirement that foreign intelligence information be the primary objective of the surveillance is plain."[144] In *Cavanagh*, the Ninth Circuit explained that "the purpose of... [foreign intelligence] surveillance is not to ferret out criminal activity but rather to gather intelligence."[145] The Ninth Circuit further held in *United States v. Sarkissian* that "[w]e have generally stated that *the purpose* of the surveillance must be to secure foreign intelligence information."[146] And in *Pelton*, the Fourth Circuit affirmed the district court's decision to approve of the surveillance activity in question because the "primary purpose of the surveillance, both initially and throughout, was to gather foreign intelligence information."[147]

In a discussion of this provision during development of the USA PATRIOT Act, Senator Leahy admitted that "even the [Justice] Department concedes that the court's [sic] may impose a constitutional requirement of 'primary purpose' based on the appellate court decisions upholding FISA against constitutional challenges over the past

---

[142] United States v. Brown, 484 F.2d 418, 424 (5th Cir. 1973).

[143] United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980).

[144] United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

[145] United States v. Cavanagh, 807 F.2d 787, 790-91 (9th Cir. 1987).

[146] 841 F.2d 959, 964 (9th Cir. 1987) (emphasis added).

[147] United States v. Pelton, 835 F.2d 1067, 1076 (4th Cir. 1987).

20 years."[148] The Senator's statement reveals the Senate's recognition and dismissal of the above circuit courts' collective conclusion regarding foreign intelligence investigations—only electronic surveillance primarily directed at gathering foreign intelligence information will be acceptable to the courts. Instead of granting due deference to the carefully considered findings of these federal courts of appeals, Congress and the Bush administration ignored clear judicial signals and created a provision that flies in the face of more than twenty years of sound case law.

Furthermore, although a number of the circuit courts have supported the finding that a FISA surveillance is not undermined simply because the agents gathered evidence that later may have proved useful as evidence in a criminal trial,[149] this conclusion is different from saying that the government may engage in surveillance for the primary purpose of obtaining evidence on which to base a criminal prosecution. The distinction is clear where an agent engages in FISA surveillance to gather intelligence information and, as a result of this authorized activity, intercepts incriminating statements that are thereupon used to support a criminal charge. This sequence of events generally has been accepted as a valid and legal corollary of a FISA surveillance.[150] Yet the courts have in no way approved of a situation where an agent conducts a FISA surveillance for the *purpose* of gathering information regarding a target's criminal activities—with an underlying secondary purpose of collecting intelligence information—and subsequently uses the intercepted statements as the foundation for bringing criminal charges against the target. By relaxing this provision of FISA concerning what an applicant for foreign intelligence

---

[148] 147 CONG. REC. S10,558 (daily ed. Oct. 12, 2001) (statement of Sen. Leahy).

[149] *See Duggan*, 743 F.2d at 78 ("[O]therwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial."); *see also Pelton*, 835 F.2d at 1076 (quoting *Duggan*); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) ("We point out that an otherwise valid FISA surveillance is not tainted because the government may later use the information obtained as evidence in a criminal trial."); *Cavanagh*, 807 F.2d at 791 ("[T]here is no merit to the contention that [the target of surveillance] is entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance not supported by probable cause of criminal activity."); *cf.* 50 U.S.C.A. § 1806(b) (West Supp. 2001) ("No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.").

[150] *See supra* note 149 (listing cases that demonstrate courts' allowance of evidence of criminal wrongdoing obtained incidentally to a FISA surveillance).

surveillance authority must demonstrate to the FISC,[151] it is conceivable that authorizations for surveillance power will be granted for the purpose of investigating primarily domestic criminal activity that has some insignificant foreign flavor, pursuant to FISA. Senator Leahy recognized that amending FISA in this way would allow for the extension of FISA-authorized surveillance for primarily criminal investigations when he indicated before the Senate: "it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of 'foreign intelligence information.'"[152] This acknowledgement is relevant in that it makes clear that the Senate foresaw the use of FISA surveillance by law enforcement agents in conducting criminal investigations—permitting an end-run around the probable cause requirement of Title III—thereby violating the Fourth Amendment rights of all targets subject to such surveillance.

It may be useful to consider the following example to understand better the infringement of Fourth Amendment privacy interests that the Senate recognized in this amendment to FISA and seemed content to allow. If a U.S. citizen of Pakistani descent is an active protestor of the World Trade Organization (WTO), an organization whose members and protestors often resort to acts of violence against merchants and politicians who support the WTO, a law enforcement agent now may seek surveillance of this individual under FISA, rather than through a Title III application. Here, the agent likely would claim a significant foreign intelligence purpose, such as investigating the individual's ties to a Pakistani group affiliated with the Taliban, while the true focus of the investigation and clear primary purpose would be a purely domestic criminal investigation of the individual's activities as a member of the anti-WTO group. This strategic use of FISA for primarily criminal investigations contravenes the statements of those courts of appeals that have addressed intelligence surveillance.[153] According to those courts, once the principal purpose of a FISA surveillance becomes a criminal investigation, a judge of competent jurisdiction must find probable cause that a serious crime has been or will be committed before surveillance may continue, as required by Title III and the Fourth Amendment.

In remarks made before the Senate, Senator Feinstein argued that

---

[151] 50 U.S.C. § 1804(a)(7)(B) (1994).

[152] 147 CONG. REC. S10,558 (daily ed. Oct. 12, 2001) (statement of Sen. Leahy).

[153] *See supra* notes 61-70, 140-47 and accompanying text (discussing cases).

amending the language of § 1804(a)(7)(B) would be advantageous, as "[t]he effect of this provision [would] be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution."[154] Although indeed there likely will be many cases where surveillance of a particular target is necessary for both criminal investigation and foreign intelligence purposes, making it easier for agents to obtain FISA authority for this type of surveillance does not outweigh the likelihood of abuses that will result from lessening the standard for receiving a FISA surveillance order. An approach that is more protective of a target's constitutional rights would require agents to obtain surveillance authority under the more stringent requirements of Title III where an investigation appears to have equal elements of a criminal investigative and a foreign intelligence gathering purpose.

Different legal standards apply to investigations for the purpose of gathering foreign intelligence information versus those for the purpose of obtaining criminal evidence. Allowing this new language of a "significant purpose" to blur that distinction is inherently problematic in that it will allow courts to apply the lesser standard of FISA surveillance to criminal investigations, without establishing pre-surveillance probable cause. When the overriding purpose of a surveillance request is unclear, preserving the privacy interests of a potentially innocent target should be a higher priority than facilitating the receipt of surveillance authority, especially considering the intrusive nature of such surveillance. It is worth noting that in analyzing these provisions one must think not only about how the USA PATRIOT Act will affect terrorists, but also how the language of the USA PATRIOT Act will apply to all Americans who find themselves under the invasive gaze of a governmental surveillance order.

B. *Allowing Primarily Criminal Investigations to Fall Within FISA Surveillance Authority Minimizes Judicial Oversight of the Criminal Investigative Process*

An additional concern arises as a consequence of amending the language of § 1804(a)(7)(B) from "purpose" to "significant purpose": if law enforcement agents take advantage of the option to bring applications for surveillance authority directed at investigations of primarily criminal activities to the FISC, this will greatly minimize judicial

---

[154] 147 CONG. REC. S10,591 (daily ed. Oct. 12, 2001) (statement of Sen. Feinstein).

oversight of criminal investigations. As discussed earlier, Title III requires the applicant for surveillance authority to demonstrate a finding of probable cause that a crime has been or will soon be committed.[155] This high threshold of proof as a condition precedent to the judge's grant of a warrant ensures that the surveillance applicant has engaged in an adequate investigation and has attained the requisite information to justify infringing the target's privacy interests. While FISA also requires a FISC judge to find certain factors set out in 50 U.S.C. § 1805, the Second Circuit in *Duggan* made clear that the role of the judge in reviewing FISA applications is minimal: "The FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information .... Thus, the representations and certifications submitted in support of an application for FISA surveillance should be presumed valid."[156] Therefore, it is clear that if law enforcement agents are given the opportunity to apply for surveillance authority intended for a primarily criminal investigation under the expanded "significant purpose" language of section 218, there will be less stringent review of the surveillance application during the initial grant of authority.

A FISC grant of authority for surveillance of criminal activities has implications beyond the initial "minimal scrutiny,"[157] as surveillance extensions under FISA serve to reduce further judicial oversight that would be provided by a Title III authorization. Under Title III, all grants of wiretap authority may continue no longer than thirty days.[158] If after the thirty-day limit the law enforcement agent conducting a given wiretap would like to prolong surveillance, he may do so only upon application for an extension.[159] This relatively short period of time allotted for surveillance of criminal suspects ensures that a neutral and detached judge will be involved sufficiently with reviewing whether the surveillance has been performed to the satisfaction of the court, as well as whether the information obtained thus far justifies

---

[155] 18 U.S.C. § 2518(3)(a) (1994).

[156] United States v. Duggan, 743 F.2d 59, 77 & n.6 (2d Cir. 1984).

[157] *Id.*

[158] *See* 18 U.S.C. § 2518(5) (1994) ("No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days.").

[159] *See id.* ("Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section.").

continuation of surveillance. If the court believes the circumstances warrant an extension, Title III provides that "[t]he period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days."[160] In contrast, FISA allows the initial surveillance to continue for up to ninety days, or one year for surveillance targeted against a foreign power,[161] thereby providing far less judicial supervision of surveillance activities. Therefore, if a law enforcement agent will be permitted to receive FISA surveillance authority for a predominantly criminal investigation under the "significant purpose" amendment to § 1804(a)(7)(B), judicial oversight of the authorized surveillance will be greatly reduced. The resulting effect will allow criminal investigations to continue from three to twelve times longer,[162] before the law permits a neutral judge to review the actions of the agents conducting the surveillance.

The foregoing analysis assumes that the reviewing court will be granted the opportunity to evaluate the authorized surveillance upon an agent's application for a surveillance extension. Because of the short duration of Title III wiretaps, it is more likely that an agent will have to apply for an extension—thereby allowing for judicial review—than with the longer duration of a FISA surveillance. With a FISC authorization of surveillance, agents may intercept all conversations of a given criminal suspect for up to three months, and if at the end of this time the agents decide not to apply for an extension, a judge will never review the actions of the agents during this extended period of time. Because FISA does not provide for notice of completed surveillance to be given to targets, a target of such surveillance may never know that his conversations had been intercepted and his privacy so completely invaded.

Amending the language of § 1804(a)(7)(B) such that a FISA surveillance now may be conducted as long as "a significant purpose of the surveillance is to obtain foreign intelligence information," disrupts FISA's balance between allowing governmental actors the ability to conduct surveillance as a means to safeguard national security, and protecting the Fourth Amendment rights of U.S. citizens to be free

---

[160] *Id.*

[161] 50 U.S.C.A. § 1805(e)(1) (West Supp. 2001); *see also* ACLU v. Barr, 952 F.2d 457, 462 (D.C. Cir. 1991) (discussing the duration of court-ordered surveillance under FISA).

[162] *See Barr*, 952 F.2d at 462 (applying the extended surveillance periods authorized by FISA).

from unreasonable searches and seizures. By changing this one word from "primary" to "significant," the USA PATRIOT Act permits the government to intrude upon the privacy of Americans without demonstrating probable cause that a crime has been or is soon to be committed—and without sufficient judicial oversight of such invasive governmental action.

C. *Roving Wiretap Authority Is Expanded to FISA Without Sufficient Privacy Protections*

In 1986, Congress amended Title III to allow for "roving wiretaps" in criminal investigations.[163] Therefore, if law enforcement agents could demonstrate to the reviewing judge that a suspect purposely was changing telephones as a means to thwart previously authorized governmental wiretaps, they could obtain a "roving" wiretap warrant—allowing agents the ability to target their surveillance on an individual, rather than a particular telephone.[164] Congress further relaxed this highly intrusive provision in 1998, by allowing roving wiretaps to be approved when the target's conduct in changing telephones has *the effect* of thwarting the electronic surveillance activities.[165] Although this amendment loosened the standard for receiving a roving wiretap, Congress included a provision requiring that law enforcement determine whether the target actually was using the phone line or was "reasonably proximate to the instrument through which such communication will be or was transmitted"[166] before wiretapping could begin—as a means of protecting an innocent conversant from unnecessary invasion of privacy. In practice, a Title III roving wiretap allows law enforcement agents to tap any telephone that the target has used or very likely will use, but only intercept those conversations when the agents reasonably believe the target is using a particular phone. Therefore, if the target of a roving wiretap uses a telephone in a coffee shop, another person's home, or an office, agents can tap that telephone for the duration of time that the warrant specifies, up to the thirty-day limit, subject to the "reasonably proximate" restraint. The Supreme Court has not addressed whether roving wiretaps violate the Fourth Amendment.

---

[163] 18 U.S.C. § 2518(11) (1994).

[164] *See* ACLU, *How the USA-PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance* (Oct. 23, 2001) (describing the 1986 amendments to Title III allowing roving wiretaps), *available at* http://www.aclu.org/congress/1102301g.html.

[165] 18 U.S.C. § 2518(11)(b)(ii) (Supp. IV 1998).

[166] *Id.* § 2518(11)(b)(iv) (Supp. IV 1998).

Section 206 of the USA PATRIOT Act serves to extend Title III's roving wiretap authority to intelligence wiretaps authorized under FISA.[167] Accordingly, if the behavior of a target has the effect of thwarting a given wiretap, the FISC may grant roving wiretap authority to the agent seeking surveillance. Advances in technology clearly justify modifying FISA to allow intelligence surveillance to meet the growing use of cellular telephones, pagers, and e-mail, all portable methods of communication that may have the effect of thwarting surveillance,[168] so that "surveillance can continue without disruption when, for example, a suspect changes cell phone numbers."[169]

Yet, the extension of roving wiretap authority to FISA raises questions regarding how this provision will be implemented, as it does not contain the "reasonably proximate" privacy protection provision of Title III. Therefore, pursuant to FISA authority, an agent now may wiretap a telephone even if it is unclear whether the target is actually using the telephone, or is reasonably close to it.[170] An agent can wiretap and listen to a phone line in an innocent individual's home for the entire day, if the agent had information that the target was expected to visit that person at some point during a given twenty-four hour period. Even if it is clear that the target already had left the location, surveillance of that telephone theoretically can continue for an unlimited period of time. This means that the private conversations of the individuals who live in this particular home, as well as the conversations of all the people they speak with on the telephone over the course of that day, will be intercepted by the government without sufficient justification.[171] If section 206 contained a protection similar to the "rea-

---

[167] *See* H.R. Res. 3162, 107th Cong. § 206 (2001) (detailing these amendments to FISA).

[168] "This authority is critical for tracking suspected spies and terrorists who are experts in counter-surveillance methods such as frequently changing locations and communications devices such as phones and computer accounts." 147 CONG. REC. S10,577 (daily ed. Oct. 12, 2001) (statement of Sen. Hatch).

[169] James Heaney, *New Anti-Terrorism Measure Inspires Passion on Both Sides; The White House Is Pushing New Legislation to Protect the Nation From Today's Sophisticated Terrorists. But Critics Suggest the Proposal Would Erode the Privacy Rights of Average Citizens*, BUFFALO NEWS, Oct. 3, 2001, at A1.

[170] Representative Scott explained that the roving wiretap provision

> means that wherever the [target] goes, whatever phone that the [target] uses, you can tap that phone, neighbors, pay phones, anybody else; and therefore you have a situation where innocent people who may also be using that phone will have their conversations listened in on. I will note that this is not limited to terrorism, and it is not even limited to criminal activity.

147 CONG. REC. H6,760 (daily ed. Oct. 12, 2001) (statement of Rep. Scott).

[171] In a discussion before the Senate, Senator Feingold gave the example that as

sonably proximate" provision as Title III affords, the government would not be able to listen to every conversation held on this phone line throughout the day, but rather only those taking place when the target is actually in that person's home. Considering the number of telephones or modes of communication a given target could use during the course of a ninety-day surveillance, it becomes clear just how many private conversations could be listened to for "intelligence" purposes.

Congress clearly recognized that section 206 will allow the government to infringe upon the privacy interests of innumerable Americans, as Senator Feingold brought this issue to the Senate's attention when he requested adding a provision similar to the protection afforded by the Title III "reasonably proximate" requirement.[172] Senator Feingold proposed amending section 206 by including:

> except that, in such circumstances, the order shall direct that the surveillance shall be conducted only when the target's presence at the place where, or use of the facility at which, the electronic surveillance is to be directed has been ascertained by the person implementing the order and that the electronic surveillance must be directed only at the communication of the target.[173]

The Senator from Wisconsin explained:

> I am not opposed to expanding existing roving wiretap authority to include FISA investigations, but I am very concerned that Section 206 does not include a key safeguard that was part of the roving wiretap authority when it was added to title III in 1986. That protection minimizes the possible misuse of the authority, whether intentional or unintentional, to eavesdrop on the conversations of individuals who are not the subject of the investigation . . . . It seems to me that Congress struck the right bal-

---

section 206 currently stands, "[i]f the government receives information that the target of the FISA investigation is making phone calls from a particular bank of pay phones in a train station, it may set up wiretaps at all the phones in that bank . . . [such that] the private conversations of innumerable innocent Americans . . . would be subject to government scrutiny." *Id.* at S10,576 (statement of Sen. Feingold). Feingold continued, "That violates their Fourth Amendment rights. Similarly, the Government should not be able to conduct surveillance on all payphones in a neighborhood frequented by a suspected terrorist or on a particular payphone all day long while innocent people use it." *Id.*

[172] *Id.* Representative Scott also requested a similar amendment to section 206 that was not accepted by the House of Representatives, which "would have required the police, when they are listening in on . . . conversations, to stop listening when the target is not using the phone. When the target leaves the organization or leaves the building, stop listening." 147 CONG. REC. H7,159 (daily ed. Oct. 23, 2001) (statement of Rep. Scott).

[173] 147 CONG. REC. S10,575 (daily ed. Oct. 11, 2001) (statement of Sen. Feingold).

> ance in that provision. It recognized the needs of law enforcement, but also recognized that rights of innocent people were implicated and designed a safeguard to protect them.[174]

Senator Feingold further explained that a protective provision similar to that found under Title III likely would not hinder intelligence or law enforcement surveillance activities under FISA, as the longstanding success of extensive and sophisticated Title III wiretaps demonstrates.[175] If the "reasonably proximate" provision of Title III wiretaps had been found to be inefficient and burdensome there would have been an effort to change it, yet there has been no such endeavor since the enactment of the provision in 1986.[176] Therefore, there is no legitimate reason why Senator Feingold's proposed amendment or a provision similar to that found in Title III should not be added to section 206's extension of roving wiretap authority to FISA surveillance.

Senator Hatch addressed Senator Feingold's remarks by stating that a provision similar to Title III's "reasonably proximate" requirement "is operationally unworkable. The way that roving orders are implemented, requires that law enforcement officers have the ability to spot check several different telephones in order to determine which one is being used by the target of the order."[177] Unfortunately, Senator Hatch's rationale for not supporting Senator Feingold's proposal seems to stem from a skewed understanding of the Wisconsin Senator's proposed amendment to section 206. Senator Feingold's suggestion would allow agents conducting a FISA surveillance to spot check any telephones that the target may be using, but only as long as the agent has *some* indication that the target is in the location where the wiretap is located and the agent reasonably believes the target is using that particular phone. Therefore, if the target visits an office, the agents conducting surveillance could intercept any conversations coming from that office while the target is present there. The agent, however, would have to cease all surveillance activities once the target had left the building, or if it is clear that the target was no longer using any phone lines. As Senator Leahy further explained, "Senator Feingold's amendment simply assures that when roving surveillance is conducted, the Government makes efforts to ascertain that the target is actually at the place or using the phone, being tapped. This is required in the criminal context. It is unfortunate that the Administra-

---

[174] *Id.* at S10,575-76.
[175] *Id.* at S10,575.
[176] *Id.* at S10,577.
[177] *Id.* (statement of Sen. Hatch).

tion did not accept this amendment."[178]

The most distressing aspect concerning the discussion of Senator Feingold's proposed amendment to section 206 was the manner in which it was hastily disregarded as a means to expedite the legislative process. Instead of allotting sufficient time to consider a provision that would safeguard the Fourth Amendment rights of countless Americans, the Senate tabled Senator Feingold's amendment in a deliberate attempt to create legislation, regardless of whether it would pass constitutional scrutiny. This point was made all too clear by Senate Majority Leader Daschle when he stated in response to Senator Feingold's proposal:

> I am sympathetic to many of these ideas, but I am much more sympathetic to arriving at a product that will bring us to a point where we can pass something into law . . . . It is too late to open up the amendment process in a way that might destroy that delicate balance [we have achieved].[179]

Furthermore, since FISA will be expanded under section 218 of the USA PATRIOT Act—such that a greater number of law enforcement agents will be likely to seek surveillance authority under the rationale that foreign intelligence gathering constitutes a "significant purpose" of the investigation—section 206 of the Act now makes receiving surveillance authority for criminal investigations under FISA even more attractive. Because the roving wiretap provision under FISA does not require that the wiretapping agent ascertain whether the target is actually using a particular telephone, a law enforcement agent can tap a telephone for lengthy periods of time in the hope of recording incriminating information from another source using that line. The potential abuses of this provision are easily foreseeable in a situation where a surveillance target lives, works, or spends time with a third party who is also suspected of involvement in criminal behavior and who uses the same telephones as the target. Under these circumstances, FISA grants the agents sufficient leeway to extend surveillance to the third party, simply by listening to the telephones that the agents believe the target and third party use. Here, individuals for whom there is insufficient information to obtain FISA authority for surveillance and inadequate information to establish probable cause as required under Title III, will be ensnared by FISA surveillance of another target, thereby greatly expanding the reaches of a FISA wiretap

---

[178] *Id.* (statement of Sen. Leahy).

[179] *Id.* (statement of Sen. Daschle).

authorization.

Although extending roving wiretap authority to FISA surveillance is clearly a necessary legislative action considering the technological advances in communications and the need for surveillance to match such developments, the USA PATRIOT Act's amendment to FISA is problematic in that it is not sufficiently tailored to protect the privacy interests of third parties whose conversations undoubtedly will be intercepted as a consequence of such poorly defined wiretap authority under section 206. Without the protection afforded by the "reasonably proximate" provision of Title III, or a similar provision such as that proposed by Senator Feingold, section 206 will allow FISA surveillance of a particular telephone line to extend for potentially unlimited and unreasonable periods of time. The result of these extended wiretaps will be the interception of nontargets' conversations, thereby unduly violating these individuals' Fourth Amendment rights against unreasonable searches and seizures. Despite the invasive nature of this surveillance activity, it is unlikely that these third parties ever could discover that the government had so fully infringed their Fourth Amendment rights. Unless the government brings charges against such parties, the unsuspecting victims never will learn of the surveillance activities.

D. *New Definition of Domestic Terrorism Will Now Describe the Activities of Many Politically Involved Americans*

Section 802 of the USA PATRIOT Act amends 18 U.S.C. § 2331, which defines international terrorism by instituting a new crime of "domestic terrorism." The Act broadly defines "domestic terrorism" as

> activities that—
>
> (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
>
> (B) appear to be intended—
>
> (i) to intimidate or coerce a civilian population;
>
> (ii) to influence the policy of a government by intimidation or coercion; or
>
> (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
>
> (C) occur primarily within the territorial jurisdiction of the United States.[180]

Upon review of this expansive definition it becomes clear that many

---

[180] 18 U.S.C.A. § 2331(5) (West Supp. 2001).

acts of political dissent and activism now will be characterized as "domestic terrorism." Such a broad definition for a wide range of underlying crimes greatly increases the number of activities that likely will fall within the USA PATRIOT Act's scope. As the definition of "domestic terrorism" stands, it encompasses activities ranging from those of anti-abortion activists who use violence against women entering Planned Parenthood clinics, to World Trade Organization protesters who throw rocks through the windows of merchants and politicians who publicly support the WTO. As Representative Paul clarified:

> Under this broad definition, should a scuffle occur at an otherwise peaceful pro-life demonstration the sponsoring organization may become the target of a federal investigation for terrorism. We have seen abuses of law enforcement authority in the past to harass individuals or organizations with unpopular political views. I hope my colleagues consider that they may be handing a future administration tools to investigate pro-life or gun rights organizations on the grounds that fringe members of their movements advocate violence. It is an unfortunate reality that almost every political movement today, from gun rights to environmentalism, has a violent fringe.[181]

By creating a new crime of "domestic terrorism" and including it in an extensive anti-terrorism act, this action makes clear Congress's and the administration's intent to use the full power of the government's surveillance capability to combat both foreign and domestic forms of terrorism. Although this is undoubtedly a necessary and important initiative, particularly in light of the events of September 11th, the language of section 802 has not been pursued in enough detail to protect against using this broad definition as a means to silence or prosecute political protestors and dissidents. As Representative Kucinich stated before the House, "It is an attack on freedom to create laws which can endanger legitimate protests."[182] Here, it is important to revisit the findings of the Church Committee, which uncovered extensive abuses of "foreign intelligence investigations" that were authorized under the pretext of protecting national security.[183]

> The Church Committee found that the FBI's internal security and domestic intelligence programs [as well as other national intelligence agencies such as the CIA and NSA] compiled massive files on activities protected by the First Amendment and the political opinions of Americans . . . . The scope of intelligence gathering swept up environmental

---

[181] 147 CONG. REC. H6,768 (daily ed. Oct. 12, 2001) (statement of Rep. Paul).

[182] *Id.* at H6,767 (statement of Rep. Kucinich).

[183] *See supra* notes 82-85 and accompanying text (discussing the Church Committee's investigation of domestic intelligence agencies).

> groups, women's liberation activists, and virtually any organization that mounted peaceful protest demonstrations.[184]

It is imperative that our laws prevent law enforcement and intelligence agents from conducting surveillance of an individual or organization based primarily on an individual's First Amendment right to exercise his or her freedom of speech and to associate with political organizations of his or her choosing.

Considering how sections 218 and 206 ease the receipt of and extension—both in length of time and to third parties—of a FISA authorized surveillance, it is likely that intelligence and law enforcement agents will seek FISA authority to conduct investigations of "domestic terrorism." Therefore, if a law enforcement or intelligence agent can demonstrate to the FISC or the Attorney General that there is *some* foreign connection to a particular activist group, such as receipt of money from an unknown foreign supporter or membership of a foreign alien, this may be sufficient for a grant of surveillance authority under FISA. Consider again the example mentioned earlier of a U.S. citizen of Pakistani descent who is an active protestor of the WTO. A law enforcement or intelligence agent may seek surveillance authorization by claiming a significant foreign intelligence purpose, such as investigating the individual's ties to a Pakistani group affiliated with the Taliban. The true focus and primary purpose of the investigation, however, would be a purely domestic criminal investigation of the individual's activities as a member of the anti-WTO group.

Although FISA explicitly provides in § 1805(a)(3)(A) that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment,"[185] the fact that a target is a member of a vocal political organization likely will play *some* role in establishing the basis for a court-ordered surveillance authorization. As long as the agent applying for surveillance authority can demonstrate some other justification beyond the target's involvement with the organization—such as being born abroad, being married to a noncitizen, or traveling to countries with which the United States does not have strong foreign relations—this may be enough to receive a grant of surveillance from the FISC. This conclusion is consistent with § 1805(b), which states that "[i]n determining whether or not probable cause exists for purposes of an order under subsection (a)(3), a judge may consider past

---

[184] 147 CONG. REC. S10,992 (daily ed. Oct. 25, 2001) (statement of Rep. Leahy).

[185] 50 U.S.C.A. § 1805(a)(3)(A) (West Supp. 2001).

activities of the target, as well as facts and circumstances relating to current or future activities of the target."[186]

Furthermore, aside from court-ordered wiretaps, FISA also empowers the Attorney General to authorize electronic surveillance without a court order.[187] Under this significant grant of authority, there is no provision prohibiting the Attorney General from granting a surveillance order based primarily on an individual's membership in a political organization. While the Attorney General must certify that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party,"[188] the fact that there is no judicial review of the Attorney General's authorization creates "the temptation to utilize such surveillances to oversee political dissent."[189] Although the Supreme Court definitively held in *United States District Court* that judicial approval must be received before conducting surveillance on a domestic organization,[190] the Attorney General authorized surveillance of the JDL in *Zweibon*, not because the government feared for the national security, but because they were concerned that JDL activities "could create a situation of international embarrassment to this country."[191] *Zweibon* illustrates the government's penchant for abusing foreign intelligence surveillance power. Any such abuse could have significant consequences for domestic political organizations, considering that so many are international in scope and that countless law-abiding Americans are politically involved with various causes.

A foreseeable and troublesome consequence of extending FISA surveillance to political protesters and activists is the infringement of Americans' constitutional right to exercise their freedom of speech—particularly when voices are raised for the purpose of political protest. In *United States District Court*, the Court foresaw the potential for abuse in situations where agents would use FISA surveillance authority to

---

[186] *Id.* § 1805(b) (West Supp. 2001).

[187] *See id.* § 1802 (West Supp. 2001) (specifying that electronic surveillance may be authorized in order to acquire foreign intelligence information if certain conditions are satisfied).

[188] *Id.* § 1802(a)(1)(B).

[189] United States v. United States Dist. Court, 407 U.S. 297, 320 (1972).

[190] *Id.* at 323-24.

[191] Zweibon v. Mitchell, 516 F.2d 594, 609 n.24 (D.C. Cir. 1975). The court discussed the Attorney General's motivation for authorizing surveillance and the lack of evidence that the surveillance achieved its purported aim of providing advance knowledge of JDL activities causing international embarrassment to the United States. *Id.* at 609.

target individuals involved with domestic political organizations:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech . . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs . . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[192]

Under federal law there are already three definitions of terrorism—international terrorism,[193] terrorism transcending national borders,[194] and federal terrorism[195]—which together sufficiently characterize the various manifestations of terrorism, including the activities perpetrated against Americans on September 11th. Therefore, it remains unclear why this fourth broad definition is necessary, especially given that it will serve to encompass the actions of political protestors. While political protest and dissent is protected under the First Amendment[196] as one of America's most cherished freedoms, the behavior is no longer shielded when protest becomes dangerous to human life.[197] Individuals who participate in protests that become violent are criminally liable and subject to either fines or serious penalties for their actions. These protests, however, are not necessarily acts of "terrorism" and therefore should not be termed as such. While violent acts of protest should not be condoned, the actions of a protestor who throws a rock through a Congresswoman's office window to demonstrate disapproval of the WTO's political agenda should not be equated with the horrific acts of terrorism that were perpetrated against the American people on September 11th.

---

[192] 407 U.S. at 313-14.

[193] 18 U.S.C. § 2331 (1994).

[194] 18 U.S.C. § 2332b (Supp. V 1999).

[195] 18 U.S.C.A. § 2332b(g)(5) (West Supp. 2001).

[196] *See* Banks & Bowman, *supra* note 33, at 86 ("Membership in, and activities in support of, an organization that advocates even the violent overthrow of the government of the United States are protected by the First Amendment, absent a showing that the person specifically intends to further the organization's unlawful objectives.").

[197] *See supra* notes 29-31 and accompanying text (discussing the courts' unwillingness to protect violent or illegal acts under the guise of freedom of expression).

CONCLUSION

After gaining a better understanding of the intrusions that sections 218, 206, and 802 of the USA PATRIOT Act will permit upon constitutionally protected civil liberties, particularly our Fourth Amendment right as American citizens "to be secure in [our] persons, houses, papers, and effects, against unreasonable searches and seizures"[198] and our First Amendment right of "freedom of speech . . . [and] the right of the people peaceably to assemble,"[199] it is clear that Americans should not be so willing to give up these valued freedoms as a means to combat terrorism. Considering the strengths of pre-USA PATRIOT Act laws, such as Title III and FISA, it is evident that these finely balanced surveillance statutes provide the government with sufficient means to investigate criminal activities and gather intelligence information necessary to safeguard national security—without unduly intruding upon the individual privacy interests of the American people. While the attacks of September 11th demonstrated a need to improve the efficiency and effectiveness of surveillance measures, there is no indication that current surveillance capabilities cannot simply be increased or enhanced without radically altering the confines of the existing authorizing laws to address terrorist threats. Instead of determining whether Title III and FISA, as they existed prior to enactment of the USA PATRIOT Act, were adequate surveillance authorities to combat the new terrorist activities, the administration strategically played upon the backdrop of September 11th to pass these new provisions that will provide the government with surveillance authority that far surpasses its needs.[200]

In supporting the passage of the USA PATRIOT Act, Senator Hatch stated, "the fact is that the bulk of these proposals have been requested by the Department of Justice for years, and have languished in Congress for years because we have been unable to muster the collective political will to enact them into law."[201] Yet, perhaps these pro-

---

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

[199] U.S. CONST. amend. I.

[200] As one opponent of the law remarked:

> This bill takes advantage of the trust that we have placed in this administration. Our law enforcement and intelligence community have all of the laws . . . that they need to do their job . . . . [T]hey failed us; and now this Attorney General is using this unfortunate situation to extract extraordinary powers to be used beyond dealing with terrorism, laws that he will place into the regular criminal justice system.

147 CONG. REC. H6,763 (daily ed. Oct. 12, 2001) (statement of Rep. Waters).

[201] *Id.* at S10,560 (statement of Sen. Hatch).

visions were never enacted into law prior to passage of the USA PATRIOT Act because before September 11th, politicians and their constituents held preserving the constitutional rights of Americans as their highest priority and most important duty. Demonstrating this marked change in the political sphere, Senator Leahy discussed efforts "made a few years ago in the Senate to provide law enforcement with greater tools to conduct surveillance of terrorists and terrorist organizations" that "would have expanded the Government's authority to conduct emergency wiretaps to cases of domestic or international terrorism and added a definition of domestic terrorism"[202] similar to the one found today in the USA PATRIOT Act. That effort was subsequently tabled. Ironically, current advocates of the USA PATRIOT Act, including then Senator Ashcroft and Senator Hatch, were among those who rejected the expansion of governmental surveillance authority. At the time, Senator Hatch stated, "I do not think we should expand the wiretap laws any further. . . . We must ensure that in our response to recent terrorist acts, we do not destroy the freedoms that we cherish."[203] While the task of protecting Americans from terrorist attacks is clearly more challenging in the wake of the September 11th attacks, the constitutional rights of Americans must be no less important to our lawmakers and ourselves in times of crisis and war than they are during times of peace. As Senator Feingold reminded the Senate:

> [T]here have been periods in our nation's history when civil liberties have taken a back seat to what appeared at the time to be the legitimate exigencies of war. Our national consciousness still bears the stain and the scars of those events: The Alien and Sedition Acts, the suspension of habeas corpus during the Civil War, the internment of Japanese-Americans, German-Americans, and Italian-Americans during World War II, the blacklisting of supposed communist sympathizers during the McCarthy era, and the surveillance and harassment of antiwar protesters, including Dr. Martin Luther King Jr., during the Vietnam War. We must not allow these pieces of our past to become prologue . . . . Now some may say, indeed we may hope, that we have come a long way since those days of infringements on civil liberties. But there is ample reason for concern. And I have been troubled in the past 6 weeks by the potential

---

[202] 147 CONG. REC. S10,366 (daily ed. Oct. 9, 2001) (statement of Sen. Leahy). The above-mentioned efforts were proposed amendments to the bill that later became the Antiterrorism and Effective Death Penalty Act of 1996, offered by Senator Lieberman in May 1995. *Id.*

[203] *Id.* (statement of Sen. Leahy).

> loss of commitment in the Congress and the country to traditional civil liberties.[204]

Keeping in mind these dark periods of American history, we must be alert to the strategic use of fears associated with the recent breach of homeland security as a means to pass controversial legislation that would not have survived constitutional scrutiny if considered only days or months prior to September 11th.

One legitimate reason for Senator Feingold's concern is the speed with which this significant piece of legislation was pushed through Congress without allowing sufficient time for the Representatives to gain a thorough understanding of these important provisions and engage in debate. As Senator Leahy admitted to the Senate during the formation of the USA PATRIOT Act, "[d]espite my misgivings, I acquiesced in some of the Administration's proposals because it is important to preserve national unity in this time of national crisis and to move the legislative process forward."[205] While national unity is certainly essential in times of crisis and war, taking the time to create amendments to the existing surveillance laws that are worded with sufficient precision to protect the constitutional rights of Americans would have been the better course for our lawmakers to take. Faced with warnings of additional terrorist assaults and the fears generated by the September 11th attacks, it is understandable that the Bush administration wanted to accelerate passage of the USA PATRIOT Act. Nevertheless, the abridged process[206] by which the Senate and House

---

[204] 147 CONG. REC. S11,020 (daily ed. Oct. 25, 2001) (statement of Sen. Feingold).

[205] *Id.* at S10,990 (statement of Sen. Leahy).

[206] As Representative Scott remarked:

> I think it is appropriate to comment on the process by which the bill is coming to us. This is not the bill that was reported and deliberated on in the Committee on the Judiciary. It came to use late on the floor. No one has really had an opportunity to look at the bill to see what is in it since we have been out of our offices. The report has just come to us. It would be helpful if we would wait for some period of time so that we can at least review what we are voting on, but I guess that is not going to stop us, so here we are.

Id. at H7,200 (statement of Rep. Scott). At the same session of the House, Representative Frank also expressed his

> deep disappointment in the procedure . . . . We now, for the second time, are debating on the floor a bill of profound significance for the constitutional structure and security of our country. In neither case has any Member been allowed to offer a single amendment. This bill, ironically, which has been given all of these high-flying acronyms, it is the PATRIOT bill, it is the U.S.A. bill, it is the stand up and sing the Star Spangled Banner bill, has been debated in the most undemocratic way possible, and it is not worthy of this institution.

bills were introduced and revised is extremely distressing, considering the momentous nature of the Act and the broad range of intelligence and criminal investigations that it will alter forever.

As Representative Goodlatte expressed to the House of Representatives, "we must be careful not to trade our personal freedoms for the promise of security. Once we have sacrificed the civil liberties that our Nation was founded on, then and only then have we allowed terrorism to defeat us."[207] Although it is unlikely that the USA PATRIOT Act's far-reaching extensions of surveillance law would have enabled the government to prevent the tragedy we witnessed on September 11th, 2001,[208] it is patently apparent how we will all pay the price of a false sense of security at the cost of cherished freedoms.

Id. at H7,206 (statement of Rep. Frank). Senator Feingold further mentioned that "the pressure to move on this bill quickly, without deliberation or debate, has been relentless." *Id.* at S11,020 (statement of Sen. Feingold).

[207] *Id.* at H6,761 (statement of Rep. Goodlatte).

[208] *See id.* at S10,366 (statement of Sen. Leahy) ("Let me be clear: No one can guarantee that Americans will be free from the threat of future terrorist attacks, and to suggest that this legislation—or any legislation—would or could provide such a guarantee would be a false promise.").