Washington and Lee Law Review

Volume 59 | Issue 3 Article 5

Summer 6-1-2002

# Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror?

Heath H. Galloway

# Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror?

Heath H. Galloway*

*Table of Contents*



---

* I would like to dedicate this Note to the memory of those lost on September 11, 2001, and to all the people lost to terrorism across the globe. I would like to thank Professor Richard Seamon, Amy King and, most of all, Sara Galloway for her tireless patience.

## *I. Introduction*

> The terrorist enemy that threatens civilization today is unlike any we have ever known .... [Terrorists] enjoy the benefits of our free society even as they commit themselves to our destruction. They exploit our openness – not randomly or haphazardly – but by deliberate, premeditated design.... [W]e are at war with an enemy who abuses individual rights as it abuses jet airliners: as weapons with which to kill Americans.[1]

> The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[2]

At 8:45 in the morning on September 11, 2001 (9-11), American Airlines Flight 11 slammed into the South Tower of the World Trade Center in New York City.[3] Twenty minutes later, as live television cameras rolled and stunned New Yorkers gazed up in disbelief, a second plane, United Airlines Flight 175, banked left and ripped through the World Trade Center's North Tower.[4] Barely forty minutes after these devastating explosions that ultimately would topple the preeminent icon of America's economic dominance, a third

---

1. *Preserving Our Freedoms While Defending Against Terrorism: Hearing on DOJ Oversight Before the Senate Comm. on the Judiciary*, 107th Cong. (2001) [hereinafter *Hearing on DOJ Oversight*] (statement of John Ashcroft, Attorney General), *available at* 2001 WL 1558164 (F.D.C.H.).

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

3. *America Attacked Tuesday September 11, 2001: Another Day of Infamy, at* http://usgovinfo.about.com/library/blattack0911.htm (last visited Oct. 9, 2002) [hereinafter *America Attacked*].

4. *Id.*

civilian jetliner, American Airlines Flight 77, barreled into the United States' military headquarters at the Pentagon.[5]

In just over an hour, terrorists crippled two of the most important symbols of American society and took the lives of nearly 3,000 people;[6] on 9-11 the horrible reality of modern terrorism found a global television audience. With nothing more imposing than box cutters,[7] nineteen single-minded zealots realized what now seem disturbingly prophetic words: "[T]he technology of transportation about the planet has advanced to a point where it has become increasingly easy to plan and implement highly destructive terrorist actions in the territory of another state."[8] Now, the dust and smoke that lingered for so long over lower Manhattan has cleared and workers have mended the gaping wound in the Pentagon, yet the true breadth of the attacks' impact on the United States is only just coming to light. For more than two centuries, the United States has stood as a nation of carefully counterbalanced laws and freedoms. However, the tragic events of 9-11 have threatened the very nature of American society and forced our nation to reset the scales and to reevaluate just how free we can afford to be.

The United States government responded quickly to 9-11, both at home and abroad. Within hours, federal buildings in Washington, D.C. closed their doors and the Federal Aviation Administration shut down U.S. airports, diverting all in-flight craft to airports in Canada.[9] Within days, President Bush issued an Executive Order calling the ready reserves of the armed forces to active duty,[10] and the Department of Justice (DOJ) initiated what Attorney

---

5. *Id.*

6. *See Latest Additions to Victims List*, AP ONLINE, Feb. 5, 2002 (noting 2,759 confirmed deaths in 9-11 terrorist attacks), *available at* 2002 WL 11688056.

7. *See, e.g., Country Responds After Terrorist Attack*, WASH. POST, Sept. 13, 2001, at C14 ("[The highjackers] were armed with . . . boxcutters – very sharp razors used to cut cardboard."); Doug Hanchett & Jessica Heslam, *Attack on America*, BOSTON HERALD, Sept. 13, 2001, at O12 ("Authorities believe Arab terrorists, possibly linked to Osama bin Laden, boarded the planes at Logan armed with either knives or boxcutters."); Niles Lathem, *Anatomy of an Atrocity*, N.Y. POST, Sept. 16, 2001, at 10 (noting that hijackers aboard American Airlines Flight 77 carried knives and boxcutters); Stephen Power & Andy Pasztor, *Aftermath of Terror: FAA Issues 3 Pages of New Requirements*, WALL ST. J., Sept. 13, 2001, at A22 (noting that FAA "banned knives 'of any length or description' from being carried on board, after reports the hijackers carried boxcutters").

8. W. Michael Reisman, *International Legal Responses to Terrorism*, 22 HOUS. J. INT'L L. 3, 4 (1999).

9. *America Attacked*, *supra* note 3.

10. Exec. Order No. 13,223, 66 Fed. Reg. 48,201 (Sept. 14, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/09/20010914-5.html. In the months following 9-11, it came to light that the executive branch also activated a cold war contingency plan that moved

General John Ashcroft would later claim to be the largest investigation ever undertaken.[11] In less than a month, the intensive cross-agency investigation into the 9-11 attacks yielded the arrest or detention of at least 614 individuals considered either suspects or material witnesses.[12]

With the nation gripped in fear, President Bush created an entirely new executive agency, the Office of Homeland Defense, and charged it with "develop[ing] and coordinat[ing] the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."[13] Then, as the reaction at home started to take shape, President Bush initiated diplomatic operations overseas to secure the arrest of the man suspected of masterminding the 9-11 attacks – Osama bin Laden.[14] When diplomacy failed to bring them to justice, the President took justice to the terrorists, and on October 7, 2001 American warplanes loosed their first satellite-guided munitions over targets in Afghanistan.[15]

The unilateral actions taken by the executive branch in the weeks and months following 9-11 were undeniably momentous and arguably unprecedented. However, it is the law of the United States that must provide the chief component of any effective program "to identify, convict, and ultimately deter, those who intend to commit violence against our people and our institu-

---

some 100 key executive officials to secret fortified locations on the east coast. *See* Amy Goldstein & Juliet Eilperin, *Congress Not Advised of Shadow Government*, WASH. POST, Mar. 2, 2002, at A01 (discussing revelation of cold war contingency plan intended to ensure functioning government if Washington attacked).

11. *See Hearing on DOJ Oversight*, *supra* note 1 (statement of John Ashcroft, Attorney General) ("We have launched the largest, most comprehensive criminal investigation in world history to identify the killers of September 11 and to prevent further terrorist attacks."). As part of this investigation, Ashcroft implemented emergency law enforcement measures allowing extended detention of immigration law violators, and ordered every United States Attorney's office to establish an Anti-Terrorism Task Force. Attorney General John Ashcroft, News Briefing at Federal Bureau of Investigation Headquarters (Sept. 18, 2001), *available at* http://www.usdoj.gov/ag/agcrisisremarks9_18.htm (last visited Dec. 2, 2001).

12. *See* Attorney General Ashcroft, News Briefing (Oct. 8, 2001) ("And since September 11, we have arrested or detained 614 persons."), *available at* http://www.justice.gov/ag/agcrisis remarks10_08.htm (last visited Nov. 9, 2002).

13. Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.

14. *See* Jesse Pesta, *Afghans May Ask Suspect in Terror Attacks to Leave; Clash of Koran, Culture*, WALL ST. J., Sept. 21, 2001, at A16 (noting that President Bush demanded that Taliban turn over terrorists and close training camps).

15. *See* Dave Moniz & Andrea Stone, *High-Tech Attacks "Baby Step One" of Campaign; First Phase Aims to Disrupt Taliban, Clear Way for Aid*, USA TODAY, Oct. 8, 2001, at 3A (noting that on October 7, 2001 American bombers dropped satellite-guided bombs on targets in Afghanistan).

tions."[16] Thus, the administration's most important reaction to 9-11 came in the form of appeals for legislative action.[17] Congress quickly heeded the executive's requests, and on October 25 the Senate passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT).[18] The next day, President George W. Bush signed PATRIOT into law, promising that the new legislation would fight terrorism without sacrificing constitutional ideals.[19]

PATRIOT moved through Congress with near record speed, outpacing the congressional reaction to the Oklahoma City bombing by several months.[20] The expediency with which the counter-terrorism legislation moved through the House and Senate was largely the product of executive prodding.[21] The

---

16. Ronald J. Sievert, *Meeting the Twenty-First Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 HOUS. L. REV. 1421, 1428 (2000).

17. *See Hearing on Anti-Terrorism Legislation Before the House Comm. on the Judiciary*, 107th Cong. (2001) [hereinafter *Hearing on Anti-Terrorism Legislation*] (statement of John Ashcroft, Attorney General) ("Today [the DOJ] seek[s] to enlist [Congress's] assistance, for we seek new laws against America's enemies, foreign and domestic."), *available at* http://www.usdoj.gov/ag/testimony/2001/agcrisisremarks9_24.htm (last visited Sept. 30, 2002).

18. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter PATRIOT].

19. *See* Ann McFeatters, *Bush Signs Anti-Terror Bill; Says Tough Law Will Preserve Constitutional Rights*, PITT. POST-GAZETTE, Oct. 27, 2001, at A6 (noting that Bush "insisted the law will preserve constitutional rights, although many critics have worried that it signals too much change and an erosion of civil liberties").

20. *See* 147 CONG. REC. S10,990 (2001) (statement of Sen. Leahy) (noting that PATRIOT passed much more quickly than legislation in response to Oklahoma City bombing). Despite "[t]he bipartisan call for a quick and forceful legislative response," Congress showed considerable restraint in drafting legislation after the Oklahoma City bombing. Note, *Blown Away? The Bill of Rights after Oklahoma City*, 109 HARV. L. REV. 2074, 2074-75 (1996) [hereinafter *Blown Away*]. This *Harvard Law Review* note has argued that the legislation passed after Oklahoma City was too cautious and that the restraint resulted in a law that was ineffective for combating terrorism. *Id.* "Many of the legislative responses proposed in the wake of the Oklahoma City bombing would have granted expanded investigatory powers to law enforcement." *Id.* at 2077.

21. *See Hearing on Anti-Terrorism Legislation*, *supra* note 17 (statement of John Ashcroft, Attorney General) (discussing need for speedy response). Attorney General Ashcroft stated:

> Mr. Chairman and members of the committee, the American people do not have the luxury of unlimited time in erecting the necessary defenses to future terrorist acts. The danger that darkened the United States of America and the civilized world on September 11th did not pass with the atrocities committed that day. They require that we provide law enforcement with the tools necessary to identify, dismantle, disrupt and punish terrorist organizations before they strike again.

*Id.*; *see also* 147 CONG. REC. S11,020 (2001) (statement of Sen. Feingold) (noting that shortly

Bush administration, through Attorney General Ashcroft, repeatedly stressed that the challenges of modern terrorism required the rapid development of an entirely new paradigm for national security efforts.[22] Ashcroft claimed that any delay in legislative action would only extend America's vulnerability.[23] Congress rewarded Ashcroft's persistence with something that prior administrations long had sought: wide latitude in the use of electronic surveillance for national security investigations.[24] It appears that the tragic reality of 9-11 has bolstered the longstanding argument in favor of increasing national security, even if such action risks diluting the freedoms guaranteed under the Constitution.[25]

---

after 9-11, Ashcroft introduced bill and "urged Congress to enact it by the end of the week. That was plainly impossible, but the pressure to move on [PATRIOT] quickly, without deliberation and debate, has been relentless ever since."); 147 CONG. REC. S10,991 (2001) (statement of Sen. Leahy) (noting "administration's request for prompt consideration").

22. *See Hearing on Anti-Terrorism Legislation, supra* note 17, (statement of John Ashcroft, Attorney General) (discussing approach to modern terrorism). Attorney General Ashcroft noted:

> Our fight against terrorism is not merely or primarily a criminal justice endeavor. It is defense of our nation and its citizens. We cannot wait for terrorists to strike to begin investigations and to take action. The death tolls are too high, the consequences too great. We must prevent first – we must prosecute second.

*Id.*

23. *See Expanding Terrorism Investigation Prosecution: Hearing Before the House Comm. on the Judiciary*, 107th Cong. (2001) (statement of John Ashcroft, Attorney General) ("Until Congress [passes] these changes, we are fighting an unnecessarily uphill battle. [W]e are today sending our troops into the modern field of battle with antique weapons. It is not a prescription for victory."), *available at* http://www.usdoj.gov/ag/testimony/2001/agcrisisremarks9_24.htm (last visited Oct. 25, 2002).

24. *See* United States v. United States Dist. Ct., 407 U.S. 297, 324 (1972) (Douglas, J., concurring) (noting "campaign of the police and intelligence agencies to obtain exemptions from the Warrant Clause of the Fourth Amendment"); *Blown Away, supra* note 20, at 2079 (noting that original Oklahoma City bills sought to expand electronic surveillance authority to terrorism-related offenses).

25. *See* Lt. Gerald F. Reimers, II, *Foreign Intelligence Surveillance Act*, 4 J. NAT'L SEC. L. 55, 75 (2000) (discussing balance between security and freedom). Lt. Reimers noted:

> The consideration [of] the relationship between the federal government's need to accumulate information concerning activities within the United States of foreign powers and the people's right of privacy as embodied in statute and the Fourth Amendment, represents, in effect, part of the federal judiciary's attempt to strike a proper balance between these two compelling, albeit not easily reconciled, interests.

*Id.* (quoting William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 104-05 (1985)); *see also* Seivert, *supra* note 16, at 1423 (noting tension "between the demand for security and demands for protection of individual rights," and that it falls to law enforcement and courts to "make real and practical decisions" to balance the competing

PATRIOT brings dramatic changes to the United States' legal landscape that belie the rapidity of the Act's creation and seriously threaten to erode citizens' civil liberties. Although provisions in PATRIOT alter the federal government's posture on a myriad of important issues from immigration to money laundering,[26] the most problematic alterations from a constitutional standpoint are those affecting national security surveillance and the sharing of information between executive agencies. First, PATRIOT loosens the already lax standards for obtaining and implementing judicially-authorized national security surveillance[27] and increases the technology available to government agents implementing such investigations.[28] Furthermore, PATRIOT permits the broad dissemination of information obtained in national security investigations among various government agencies.[29] Taken as a whole, PATRIOT provides more than just the tools necessary to fight terrorism; it provides the key components to a twenty-first century Orwellian nightmare.[30]

---

interests); Mark G. Young, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1018 (2001) ("In the wake of the tragedy of September 11, the attitude towards the propriety of widespread surveillance seems to have markedly changed.").

26. PATRIOT, *supra* note 18, §§ 411-20, 115 Stat. at 356-63 (Enhanced Immigration Provisions); *id.* §§ 311-30, 115 Stat. at 298-320 (International Counter Money Laundering and Related Measures).

27. *See id.* § 218, 115 Stat. at 291 (amending Foreign Intelligence Surveillance Act (FISA) to permit warrant when foreign intelligence is "a significant purpose" as opposed to "the purpose" of investigation); *see also infra* notes 171-82 and accompanying text (discussing relaxed standard of probable cause and judicial review under FISA).

28. *See* PATRIOT, *supra* note 18, §§ 206-07, 115 Stat. at 282-83 (allowing roving FISA wiretaps); *id.* §§ 214, 216, 115 Stat. at 286-90 (allowing FISA pen register and "trap and trace" orders).

29. *See id.* § 203, 115 Stat. at 278-81 (authorizing sharing of information among law enforcement and intelligence agencies of federal government).

30. Although an allusion to *1984*'s Big Brother may seem a bit of a stretch, the actions of DOJ in recent months, such as the decision to begin monitoring attorney-client conversations and religious and political groups, suggest the allusion may not be that far off the mark. *See infra* note 32 (discussing latest executive policy changes). Furthermore, the Bush administration, through the Defense Advanced Research Projects Agency, or DARPA, has begun funding a program called Total Information Awareness that bears disturbing similarities to Orwell's fiction. *See* Nicholas Kulish & Ann Davis, *White House Defends Information-Awareness Plan*, WALL ST. J., Nov. 21, 2002, at A4 (discussing response of Bush administration to critics of proposed program); Jonathan Turley, *Government Creating Database to Track Citizens: Where is the Outcry Against this Massive Surveillance System*, CHAR. OBSERVER, Nov. 21, 2002, at 17A (discussing program and noting that "it now appears that Orwell is busy at work in the darkest recesses of the Bush administration and its new Information Awareness Office"). "As envisioned, the system which remains several years from implementation, would sift through large quantities of data . . . to try to identify potential terrorist activity." Kulish & Davis, *supra*. Allegedly the world's largest computer database, the system could have "the ability to track

At the time of this writing, PATRIOT is barely four months old, and yet the Bush administration is seeking still greater legislative fiat[31] and is taking further unilateral actions that undoubtedly will trouble many civil libertarians.[32] The Bush administration's efforts to combat terrorism vividly illustrate "the Executive's proclivity for occupying the power vacuums that result from the ponderous nature of the legislative and judicial processes."[33] Although the

---

every credit card purchase, travel reservation, medical treatment and common transaction by every citizen in the United States." Turley, *supra*. Some critics of the program have already suggested that Total Information Awareness could easily see use in areas beyond terrorism and, for instance, "might rapidly evolve into a tool to fight drug trafficking." Kulish & Davis, *supra*. This is a proposition the reader should keep in mind when considering Part IV.B.1 of this Note.

Several provisions in PATRIOT not discussed in this Note also dramatically augment the governmental surveillance of United States citizens. For instance, the Act expands the classification of domestic terrorism to an extent that could saddle a large number of domestic political groups with the damning designation of terrorist organization. *See* PATRIOT, *supra* note 18, § 802, 115 Stat. at 376 (revising definition of domestic terrorism); JOHN W. WHITEHEAD & STEVEN H. ADEN, FORFEITING "ENDURING FREEDOM" FOR "HOMELAND SECURITY": A CONSTITUTIONAL ANALYSIS OF THE USA PATRIOT ACT AND THE JUSTICE DEPARTMENT'S ANTI-TERRORISM INITIATIVES 13 (2002) (Rutherford Institute White Paper) ("Conceivably, these extensions of the definition of 'terrorist' could bring within their sweep diverse domestic political groups which have been accused of acts of intimidation or property damage such as Act Up, PETA, Operation Rescue, and the Vieques demonstrators." (citation omitted)), *available at* http://www.rutherford.org/documents/pdf/tri_analysis_of_usa_pat_act.pdf (last visited July 28, 2002). In considering the significance of this expansion, we must remember that "[d]efinitions of terrorism are particularly outcome sensitive precisely because they tend to delimit the range of lawful responses to them." Reisman, *supra* note 8, at 9.

31. *See* Clyde Haberman, *A Nation Challenged – An Overview: Nov 30, 2001, Expanded Spy Powers, Post-Taliban Bickering, An Anthrax Clue*, N.Y. TIMES, Dec. 1, 2001, at B1 (discussing administration's attempts to augment surveillance authority); Jim McGee, *Bush Team Seeks Broader Surveillance Powers: Congress Asked to Remove Legal Restrictions on CIA, FBI Ability to Intercept Suspects' Communications*, WASH. POST, Dec. 2, 2001, at A25 (same).

32. For instance, the administration invoked a policy change that gives federal agents authority to eavesdrop on certain conversations between suspected terrorists and their attorneys. *See* George Lardner, Jr., *ABA Urges Ashcroft to Kill Order*, WASH. POST, Jan. 4, 2002, at A10 (noting that on October 31, 2001, Ashcroft issued order permitting government to "listen in on talks between lawyers and clients"). President Bush signed a Military Order allowing the trial of foreign terrorist suspects before military tribunals instead of referring such cases to federal courts. Military Order of November 13, 2001, 66 Fed. Reg. 57,833 (Nov. 13, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/11/20011113-27.html. In perhaps the most troubling response, the Federal Bureau of Investigation (FBI) has begun rethinking surveillance guidelines – enacted in response to the Hoover era – largely disallowing the investigation of religious and political groups. *Ashcroft Seeking to Free F.B.I. to Spy on Groups*, N.Y. TIMES ONLINE, Dec. 1, 2001, *available at* http://tiger.berkeley.edu/sohrab/politics/fbi_spying.html (last visited July 27, 2002).

33. 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,

administration is almost certainly taking these steps in good faith and with the best of intentions, "[e]xperience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent."[34]

Congress has grown increasingly wary of executive efforts to combat terrorism and has held hearings to consider whether the Bush administration's response to the terrorist threat is in accordance with the ideals of our free democratic society.[35] This Note argues that Congress's apprehension is well advised but perhaps belated; PATRIOT may already have gone too far. While Congress considered PATRIOT, there was testimony that the enhanced surveillance authority granted under the statute, coupled with the disintegration of the wall that traditionally has separated intelligence services from law enforcement communities, presents a credible threat to the protections guaranteed by the Fourth Amendment.[36] This Note addresses certain provisions within PATRIOT affecting surveillance law and the sharing of information between the law enforcement and intelligence communities and seeks to ascertain the validity of these constitutional concerns.

This Note contends that PATRIOT provides the executive branch with tremendous flexibility over the implementation of electronic surveillance for national security purposes, and that this leeway could result in a circumvention of the Fourth Amendment in a wide range of criminal prosecutions.[37] This

---

795 (1989).

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

35. *See Preserving Freedoms While Fighting Terrorism: Hearing Before the Senate Judiciary Comm.*, 107th Cong. (2001) [hereinafter *Preserving Freedoms*] (statement of Sen. Patrick Leahy) (noting oversight committee's duty to examine actions by executive and that "[a]s with several of the unilateral steps announced by the administration over the last month, a question that puzzles many about the order on military tribunals is this: What does it really gain us in the fight against terrorism?"), *available at* 2001 WL 1563893 (F.D.C.H.); John Lancaster, *Hearings Reflect Some Unease with Ashcroft's Legal Approach*, WASH. POST, Dec. 2, 2001, at A25 (discussing congressional concern over Bush administration's efforts to fight terrorism).

36. *See Protecting Constitutional Freedoms in the Face of Terrorism: Hearing Before the Senate Judiciary Subcomm. on Constitution, Federalism, and Property Rights*, 107th Cong. (2001) [hereinafter *Protecting Constitutional Freedoms*] (statement of Jerry Berman, Executive Director, Center for Democracy & Technology) ("PATRIOT Act tear[s] down the 'wall' between the government's authority to conduct counter-intelligence surveillance against foreign powers and terrorist groups, and its authority to conduct criminal investigations on Americans."), *available at* http://judiciary.senate.gov/oldsite/tc100301sc_berman.htm (last visited Oct. 25, 2002).

37. Although not specifically addressed herein, the consequences of this end-around could be particularly perilous in national security domestic surveillance in which Fourth Amendment principles in the context of the First Amendment right of free speech are likely implicated. *See* United States v. United States Dist. Ct., 407 U.S. 297, 313-14 (1972) (discussing First and Fourth Amendment values). The Court noted:

Note further suggests that the new paradigm urged by the executive and codified in PATRIOT is incongruous with the principles underlying the Supreme Court's decisions regarding national security surveillance and discards the Foreign Intelligence Surveillance Act's (FISA)[38] carefully crafted constitutional balance.[39] Ultimately, this Note asserts that PATRIOT could result in constitutional sacrifices that contravene our democratic principles and undermine the foundation of our free society, granting the twisted terrorist minds behind 9-11 an utterly undeserved measure of victory.[40]

This Note consists of three primary parts. Part II considers Fourth Amendment jurisprudence regarding electronic surveillance, focusing in particular on those cases leading to the surveillance procedures codified in FISA.[41] In so doing, Part II illuminates the principles that have guided federal courts in evaluating surveillance procedures and considers the circumstances under which the courts have allowed and disallowed intrusions upon personal autonomy and privacy. Part II also considers the judiciary's deference to executive policy in the realm of national security and the role this approach will play as PATRIOT faces inevitable challenges in the courts.[42]

---

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security."

*Id.*

38. 50 U.S.C. §§ 1801-62 (2001).

39. *See* Reimers, *supra* note 25, at 70 (noting that FISA "check[s]" executive branch and that "[w]hat before was all but exclusive executive branch turf was divided in all three and thereby 'balanced'").

40. *See* Sievert, *supra* note 16, at 1423 ("Some terrorists hope to provoke a response that undermines our Constitutional system of government. So U.S. leaders must find the appropriate balance by adopting counterterrorism policies which are effective but also respect the democratic traditions which are the bedrock of America's strength." (quoting NAT'L COMM'N ON TERRORISM, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM, H.R. DOC. NO. 106-250, at 6 (2000))); *see also* WHITEHEAD & ADEN, *supra* note 30, at 1 ("We will not allow this enemy to win the war by changing our way of life or restricting our freedoms." (citing *President Bush's Remarks*, WASH. POST, Sept. 12, 2001, at A2)), *available at* http://www.rutherford.org/documents/pdf/tri_analysis_of_usa_pat_act.pdf (last visited Oct. 21, 2002).

41. Several commentators have taken a more in-depth look at the constitutional ramifications of government sponsored surveillance. For an excellent overview of government surveillance technologies and practices and the constitutional ramifications thereof, see Young, *supra* note 25.

42. *See* 147 CONG. REC. S10,990 (2001) (statement of Sen. Leahy) ("[S]ome of the provisions contained both in this bill and the original USA Act will face difficult tests in the

Part III considers the structure and history of FISA before the enactment of PATRIOT and the constitutional challenges to that structure. Part III also addresses the development of the historic "wall" separating the law enforcement community from intelligence agencies. This discussion considers first how the wall dividing these two entities came about, and second, how the policy became incorporated in the original structure of FISA. Finally, Part III explores and introduces factors that have blurred the line between law enforcement and intelligence operations and have led to the erosion of the wall in recent years.

Part IV examines several key provisions within PATRIOT against the backdrop of the discussions set forth in Parts II and III. First, Part IV explores PATRIOT's new surveillance measures and the modifications it brings to existing surveillance law, particularly to FISA. Second, Part IV considers the statutory grant of authority to share information among executive agencies and the likely implications of this new policy with respect to evidence obtained through FISA surveillance. Part IV also addresses the possible implementation of PATRIOT outside the realm of terrorism. Finally, Part IV argues that PATRIOT is far more sweeping than the administration would have us believe[43] and will affect criminal investigations entirely unrelated to terrorism.[44] This Note chiefly contends that the changes to FISA remove the Act from the constitutional strictures established by the federal judiciary, and that this removal – coupled with increased dissemination of information among agencies and limited executive accountability – presents a specific, realistic threat to American civil liberties.

This discussion, particularly Part IV, is limited by the novelty of the legislation and the ongoing development of pertinent issues. However, dramatic indicators of the direction in which the administration intends to take PATRIOT exist, and these indicators will serve to guide this inquiry. This Note ultimately aims to ascertain whether PATRIOT is a necessary evil, spawned from the realities of combating the modern terrorist threat in today's global environment, or whether the threat to constitutional rights is simply too great.

---

courts.").

43. *See Homeland Defense: Hearing Before the Senate Comm. on the Judiciary*, 107th Cong. (2001) (testimony of Attorney General Ashcroft) ("Each action taken by the Department of Justice . . . is carefully drawn to target a narrow class of individuals – terrorists. Our legal powers are targeted at terrorists. Our investigation is focused on terrorists. Our prevention strategy targets the terrorist threat."), *available at* http://www.senate.gov/%7Ejudiciary/testimony.cfm?id=108&wit_id=42 (last visited Sept. 30, 2002).

44. *See* 147 CONG. REC. S10,991 (2001) (statement of Sen. Leahy) ("Indeed, this bill will change surveillance and intelligence procedures for all types of criminal and foreign intelligence investigations, not just for terrorism cases.").

Before I begin, it is important to recognize somberly the depth of the wound 9-11 inflicted upon our nation. The images broadcast across the world on that Tuesday morning will forever be a traumatic component of our collective consciousness. Undoubtedly, there are those who will see any challenge to the government's efforts to combat terrorism as unpatriotic or un-American; some may even consider this commentary "ammunition to America's enemies, and pause to America's friends."[45] However, even the staunchest proponents of PATRIOT agree that "American rights and freedoms . . . must be preserved throughout this war on terrorism."[46] It would seem surprising, then, that anyone seriously would oppose an effort to ensure that the United States wages this new war with "a total commitment to protect the rights and privacy of all Americans and the constitutional protections we hold dear."[47] Thus, as I endeavor to participate in "honest, reasoned debate; not fearmongering,"[48] I take great comfort in the knowledge that I may do so "without people questioning [my] patriotism, seriousness or opposition to bad guys."[49]

## *II. Judicial Framework for National Security Electronic Surveillance*

### *A. Surveillance and the Fourth Amendment*

The swiftness with which the world became aware of the 9-11 tragedy evidences the gargantuan capabilities of modern communication technology. Every day, we become more and more intertwined, perhaps inextricably, with communication and information technology.[50] All elements of society – savory and otherwise – have begun to take advantage of the dramatic innovations that now are so frequent that they receive little notice. Just as this technology has allowed for the rapid and widespread dissemination of information, it equally has facilitated the clandestine accumulation of information.[51] Electronic surveillance has become a crucial tool for modern law

---

45. *Hearing on DOJ Oversight, supra* note 1 (statement of John Ashcroft, Attorney General).

46. *Hearing on Anti-Terrorism Legislation, supra* note 17 (statement of John Ashcroft, Attorney General).

47. *Id.*

48. *Hearing on DOJ Oversight, supra* note 1 (statement of John Ashcroft, Attorney General).

49. *Protecting Constitutional Freedoms, supra* note 36 (statement of Grover Norquist, President, Americans for Tax Reform).

50. *See* Young, *supra* note 25, at 1024-25 (discussing prevalence of communications technology in all aspects of life in United States).

51. *See Blown Away, supra* note 20, at 2088-89 ("Modern technology has made the accumulation of sensitive personal information startlingly easy." (citing GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 217-29 (1988); Matthew M. Kleiman,

enforcement and intelligence gathering;[52] both law enforcement and intelligence services continuously have sought faster, subtler, and more effective means to gather information about suspected evil-doers.[53]

Courts have struggled to stay abreast of the competing advancements in communication and surveillance technology. Unfortunately, judicial efforts to reconcile the capabilities of modern technology with traditional Fourth Amendment values have done little to dismantle the longstanding, palpable tension that developed between efforts to protect our nation and endeavors to safeguard the individual liberties guaranteed under the Constitution.[54] This tension is particularly pronounced in the protracted and exceedingly opaque jurisprudence regarding the Fourth Amendment's application to electronic surveillance.[55] Although an in-depth historical consideration of the Fourth Amendment is beyond the scope of this Note,[56] an understanding of the prin-

---

Comment, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1176-78 (1992))).

52. *See* Young, *supra* note 25, at 1025 ("[T]he prevailing view is aptly summarized by one hornbook which states: 'Wiretapping and eavesdropping are among the most effective techniques available to combat crime.'" (quoting CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING 1:1, at 1-3 (2d ed. 1995))).

53. *See id.* (providing overview of sophisticated array of surveillance technologies available to law enforcement and intelligence communities).

54. *See* United States v. Butenko, 494 F.2d 593, 596 (3d Cir. 1974) (en banc) ("Among the more perplexing dilemmas faced by a democratic society is that of securing its territorial and institutional integrity, while at the same time, preserving intact the core of liberties essential to its existence as an association of truly free individuals."); *see also* Reimers, *supra* note 25, at 75 (discussing judiciary's attempt to balance privacy rights with government's need for information). Lt. Reimers noted:

> The consideration [of] the relationship between the federal government's need to accumulate information concerning activities within the United States of foreign powers and the people's right of privacy as embodied in statute and the Fourth Amendment, represents, in effect, part of the federal judiciary's attempt to strike a proper balance between these two compelling, albeit not easily reconciled, interests.

*Id.* (citation omitted); Sievert, *supra* note 16, at 1422 (noting that courts are arbiters between competing demands for security and protection of individual liberties); Young, *supra* note 25, at 1019-20 (noting opposing reactions to 9-11 "illustrate the battle as old as the country over the proper balance between granting the government authority to maintain order in society and restraining the government from intruding on personal liberties").

55. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757-58 (1994) ("The Fourth Amendment today is . . . a vast jumble of judicial pronouncements that is not merely complex and contradictory, but often perverse. Criminals go free, while honest citizens are intruded upon in outrageous ways with little or no real remedy.").

56. This Part draws extensively from Americo R. Cinquegrana's excellent article: *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, *supra* note 33. The reader can find a more thorough treatment of the development of Fourth Amendment jurisprudence leading up to FISA therein. *See* Sievert,

ciples underlying the federal judiciary's Fourth Amendment decisions pertaining to electronic surveillance is vital to a proper evaluation of PATRIOT. Further, FISA is a direct descendant of this case-law,[57] and as this Note discusses in Part IV, the changes to this important statute present PATRIOT's chief constitutional hazard.[58] Finally, tracing the inability of the law to keep up with technological advances that refuse to slow down emphasizes the magnitude of the challenge our nation faces in trying to wage a war against modern terrorism without sacrificing essential American ideals.[59]

### *B. Early Judicial Reactions to Electronic Surveillance: From* Olmstead *to* Katz*; From Property to Privacy*

Throughout the first quarter of the twentieth century, the executive branch of the federal government utilized wiretaps and electronic listening devices without warrants as an effective method for discovering and combating criminal activity, as well as for gathering intelligence information.[60] The issue of whether such activity comported with the Fourth Amendment's prohibition on unreasonable searches and seizures did not come before the Supreme Court until 1928, in *Olmstead v. United States*.[61] Therein, the Justices considered

---

*supra* note 16, at 1428 (considering complications arising from meeting challenge of modern terrorism under strictures of traditional Fourth Amendment notions); Young, *supra* note 25, at 1017-95 (providing in-depth account of United States surveillance technologies and constitutional issues associated therewith).

57. *See* Cinquegrana, *supra* note 33, at 803 ("[T]he Court's explanation . . . regarding the flexibility that would be permissible under the [F]ourth [A]mendment paved the way for FISA and its carefully tailored provisions for surveillance of foreign powers and their agents in the United States."); Sievert, *supra* note 16, at 1436-37 (discussing Supreme Court's implicit invitation to Congress to pass legislation governing national security surveillance procedures in *Keith* and noting that "Congress accepted the Court's invitation and passed FISA").

58. *See infra* Part IV (discussing changes PATRIOT brings to FISA).

59. *See* Young, *supra* note 25, at 1020 (commenting on "the potential risks facing our society, given increasingly sophisticated technologies, and given our substantial and growing dependence on communications, transactions, and other activities which leave some kind of data trail").

60. *See* Cinquegrana, *supra* note 33, at 795 (discussing executive use of wiretaps in early twentieth century America).

61. *See* Olmstead v. United States, 277 U.S. 438, 464-65 (1928) (holding Fourth Amendment inapplicable to wiretaps). In *Olmstead*, the Supreme Court considered whether evidence obtained by wiretapping violated the Fourth and Fifth Amendments. *Id.* at 455. The Court carefully reviewed prior holdings on the Fourth Amendment and the Amendment's history. *Id.* at 458-64. The Court found that the Fourth Amendment applied to material things, such as a house, papers, etc., but that "[t]he language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office." *Id.* at 464-65. According to the majority, while Congress could establish such protection, the courts could not. *Id.* at 465-66. Therefore, the Court concluded "that the wire

whether evidence from telephone conversations, surreptitiously intercepted by law enforcement officials without a warrant, was admissible in a criminal trial.[62] In a harbinger of things to come, the issue deeply divided the Court.[63] Ultimately, the Justices endorsed a textual interpretation of the Fourth Amendment and refused to extend its protection to wiretaps.[64] In a five-to-four decision, the Court admitted the Government's evidence and effectively "removed electronic surveillance techniques not involving physical intrusions from [F]ourth [A]mendment scrutiny for almost ten years."[65]

The decision in *Olmstead*, while facilitating the executive's continued use of warrantless surveillance, also piqued the interest of Congress in regulating the procedure for obtaining surveillance authorization.[66] In 1934, Congress passed the Federal Communications Act, making the "interception and

---

tapping [in question] did not amount to a search or seizure within the meaning of the Fourth Amendment." *Id.* at 466. In a strong, progressive dissent, Justice Brandeis noted the hypocrisy of the Court's holding considering the Court's willingness to endorse an expansive reading of the Constitution with respect to the exercise of power by Congress. *Id.* at 471-72 (Brandeis, J., dissenting). According to Brandeis, the Fourth Amendment's protection must evolve with the world around it. *Id.* at 473 (Brandeis, J., dissenting). For Justice Brandeis, "[t]he evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails." *Id.* at 475 (Brandeis, J., dissenting). Therefore, concluded Brandeis, the Court should have found the government's wiretaps to be in violation of the Fourth Amendment. *Id.* at 488 (Brandeis, J., dissenting).

62. *See id.* at 455 (noting issue as "whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments").

63. *See* Cinquegrana, *supra* note 33, at 795 (noting that "Olmstead resulted in a sharp 5-4 division").

64. *See Olmstead*, 277 U.S. at 464 (refusing to interpret Fourth Amendment as protecting defendant from warrantless wiretapping). The majority stated:

> The language of the amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. . . . Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.

*Id.* at 465-66. In dissent, Justice Brandeis pointed to the hypocrisy of the majority opinion when contrasted with the Court's willingness to sustain "the exercise of power by Congress, under various clauses of [the Constitution], over objects of which the Fathers could not have dreamed." *Id.* at 472 (Brandeis, J., dissenting). Brandeis asserted that the constitutional protections of individual liberties "must have a similar capacity of adaptation to a changing world." *Id.* (Brandeis, J., dissenting).

65. Cinquegrana, *supra* note 33, at 796.

66. *See id.* (noting that decision in *Olmstead* "stir[red] congressional interest in regulating the technique [of electronic surveillance] and broadening individual protections").

disclosure of any wire or radio communication" illegal.[67] Although the legislation barred the introduction of electronic surveillance evidence in a criminal trial, it did little to halt the practice of warrantless surveillance because the executive regarded the statute, and the Supreme Court's interpretation of it, as "preventing [the] use of electronic surveillance only when it was combined with disclosure of its fruits outside of the government."[68] Congress's first attempt to curb executive surveillance thus proved wholly inadequate and the unchecked wiretapping continued.[69]

Although there were tangential judicial encroachments,[70] it was not until 1967, when the Supreme Court reevaluated the electronic surveillance issue in *Katz v. United States*,[71] that the executive's autonomy endured any real constraint.[72] *Katz* gave the Court an opportunity to reconsider its traditional

---

67. *Id.* at 797 (citing The Federal Communications Act of 1934, ch. 652, Pub. L. No. 73-416, 48 Stat. 1064, 1103-04 (1934) (codified as amended at 47 U.S.C. § 605 (Supp. III 1985))).

68. *Id.*

69. *See id.* at 799 ("[A]lmost 7000 wiretaps and 2200 microphone surveillances were used by the Executive between 1940 and the mid-1960s in internal security investigations . . . as well as major criminal activities.").

70. *See* Silverman v. United States, 365 U.S. 505, 509-12 (1961) (finding that electronic eavesdropping accomplished by "spike microphone" violated Fourth Amendment).

71. 389 U.S. 347 (1967).

72. *See* Katz v. United States, 389 U.S. 347, 358-59 (1967) (holding warrant precondition to electronic surveillance under Fourth Amendment). In *Katz*, the Court considered the constitutional questions presented by the denial of a defendant's motion to suppress evidence of conversations obtained by the FBI by means of "an electronic listening and recording device attached to the outside of the public telephone booth from which [the defendant] had placed his calls." *Id.* at 348-49. The Court first dismissed both the prosecution's suggested construction of the Fourth Amendment in terms of a "constitutionally protected area" and the defendant's idea that the Fourth Amendment "translate[s] into a general constitutional 'right to privacy.'" *Id.* at 350-51. Instead, the Court asserted that "the Fourth Amendment protects people, not places" and that what one "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351-52. The Court concluded that the Government's actions in "electronically listening to and recording the [defendant'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." *Id.* at 353. Thus, according to the Court, the issue was "whether the search and seizure . . . complied with constitutional standards." *Id.* at 354. The Court concluded that had the Government applied for a warrant, a court likely would have authorized the surveillance. *Id.* 354-56. However, that fact was insufficient to excuse the absence of authorization by a "neutral magistrate." *Id.* at 356. According to the Court, surveillance without "adherence to judicial processes" and "prior approval by a judge or magistrate, are per se unreasonable under the Fourth Amendment." *Id.* at 357 (citations omitted). Because the Government did not obtain such neutral authorization, the Court concluded that the surveillance in question violated the Fourth Amendment. *Id.* at 358-59. In footnote 23, the majority expressly declined to address whether the ruling applied with equal force to "situation[s] involving the national security." *Id.* at 358 n.23.

property rights based interpretation of the Fourth Amendment in light of the emerging threat to civil liberties posed by modern surveillance technologies.[73] *Katz* was a turning point in Fourth Amendment jurisprudence that ultimately would lay the foundation for the modern statutory approach to both criminal and national security surveillance procedures.[74]

Writing for the majority, Justice Stewart overruled the *Olmstead* trespass requirement and announced an entirely new paradigm for delineating the Fourth Amendment's protections. Although conceding that the Constitution does not guarantee a general right to privacy,[75] Stewart nevertheless opined that it protects some expectations of privacy:

> For the Fourth Amendment protects people, not places. *What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.*[76]

Justice Stewart concluded that the non-invasive electronic surveillance with which the Government surreptitiously acquired its evidence was a search and, as such, was subject to the reasonableness requirement of the Fourth Amendment.[77] With *Katz*, the Court expanded the Fourth Amendment's protections to account for the new capabilities of surveillance technology.

Once the Court identified the Government's conduct as a "search," the question remained whether the search was reasonable.[78] The Court found the search unreasonable, grounding its decision, in part, on the constitutional mandate that some judicial interposition exist between "citizens and the police."[79] The Court explicitly refused to validate the Government's actions retroactively, despite the fact that the surveillance at issue likely deserved a proper warrant.[80] Echoing the principles underlying the Court's other then-

---

73. *See* Cinquegrana, *supra* note 33, at 800 (discussing *Katz*).

74. *See id.* at 800-01 ("In enacting Title III of the Omnibus Crime Control and Safe Streets Act, Congress drew upon principles discussed in the *Katz* decision."); *id.* at 800 ("The Court's gratuitous discussion in *Katz* regarding surveillance activities undertaken in furtherance of national security interests was critical to the development of FISA.").

75. *Katz*, 389 U.S. at 350.

76. *Id.* at 351 (citations omitted) (emphasis added).

77. *See id.* at 353 (finding Government's actions to be "'search and seizure' within the meaning of the Fourth Amendment").

78. *Id.* at 354.

79. *Id.*

80. *See id.* at 356-57 (noting that magistrate would have accommodated Government's "carefully limited" surveillance, but that because Government obtained no such order, surveillance violated Fourth Amendment).

recent Fourth Amendment decisions,[81] Justice Stewart found the Government's self-imposed restraint an inadequate safeguard and refused to justify a search "upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end."[82] The Court drew a line in the sand and declared that any search conducted without prior judicial approval would be "*per se* unreasonable under the Fourth Amendment,"[83] except in certain specific situations.[84]

Justice Stewart's pronouncement was momentous in that it provided the first principle for determining the constitutionality of government surveillance: the presence of prior judicial authorization. However, the most important facet of *Katz* for purposes of this Note is not in the text of the opinion itself, but in footnote 23 and in the concurring opinions of Justices Douglas and White.[85] Justice Stewart's footnote excluded national security surveillance from the rule of law fashioned in his opinion, explicitly leaving open the question of what Fourth Amendment principles should apply to such situations.[86]

The ambivalence of the footnote 23 disclaimer did not sit well with some of Justice Stewart's peers. On the one hand, Justice Douglas felt that the footnote provided an "unwarranted green light for the executive branch to resort to electronic eavesdropping without a warrant in cases which the executive branch itself labels 'national security' matters."[87] On the other hand, Justice White believed the majority opinion did not go far enough and that the Court should endorse affirmatively an exception to the Fourth Amendment for

---

81. *See* Johnson v. United States, 333 U.S. 10, 13-14 (1948) (discussing Fourth Amendment protections). The *Johnson* Court noted:

> The point of the Fourth Amendment . . . is not that it denies law enforcement the support of the usual inference which reasonable men draw from the evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.

*Id.*

82. Katz v. United States, 389 U.S. 347, 357 (1967).

83. *Id.* at 357.

84. National security was conspicuously absent from the exceptions noted by Justice Stewart. *See id.* at 357-58 (noting electronic surveillance unlikely to be incident to arrest and unjustifiable on grounds of hot pursuit).

85. *See* Cinquegrana, *supra* note 33, at 800 (noting footnote 23 and concurrences as "critical to the development of FISA").

86. *See Katz*, 389 U.S. at 358 n.23 ("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.").

87. *Id.* at 359 (Douglas, J., concurring).

the President and the Attorney General when acting in the interests of national security.[88] The sharp division in the Court regarding the principles applicable in the national security context was a portent; only five years later, the Justices addressed the issue directly.

However, before the Court returned to the issue of national security surveillance, Congress reacted to the *Katz* decision with another attempt to regulate executive surveillance: Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[89] Congress intended Title III to provide the framework for obtaining court-ordered surveillance authority in criminal investigations; it "represent[ed] a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression."[90] In Title III, Congress set forth an elaborate probable cause requirement such that a warrant for electronic surveillance could issue only when the reviewing judge:

> [D]etermine[d] on the basis of the facts submitted by the applicant that –
> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;
> (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
> (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
> (d) except as provided in subsection (11), there is probable cause to believe that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.[91]

---

88. *See id.* at 364 (White, J., concurring) ("We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.").

89. Omnibus Crime Control and Safe Streets Act of 1967, Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)); *see* United States v. United States Dist. Ct., 407 U.S. 297, 302 (1972) (noting that "[m]uch of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in . . . Katz v. United States, 389 U.S. 347 (1967)"); Cinquegrana, *supra* note 33, at 800-01 ("In 1968, Congress accepted the judicial and executive invitation, outstanding since *Olmstead*, to define more clearly the proper use of electronic surveillance techniques in criminal investigations. In enacting Title III of the Omnibus Crime Control and Safe Streets Act, Congress drew upon principles discussed in the *Katz* decision.").

90. United States v. United States Dist. Ct., 407 U.S. 297, 302 (1972).

91. 18 U.S.C. § 2518(3) (2000).

Unfortunately, Congress also was unwilling to weigh in conclusively on the applicability of the Title III standard to executive surveillance for national security[92] and reiterated the *Katz* Court's deference:

> 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.[93]

Not surprisingly, the executive branch interpreted the Title III disclaimer, together with the *Katz* Court's implicit exclusion of national security measures, as allowing total executive autonomy in devising and implementing surveillance procedures for internal security missions; the executive reasoned that in such situations the carefully crafted principles governing criminal surveillance simply did not apply.[94] In effect, Congress and the Court "perpetuated the ability of the executive branch to occupy the field and conduct electronic surveillance without prior judicial review when [it] deemed necessary."[95]

### C. *The* Keith *Case and Lower Court Interpretations: Framing the Foreign Intelligence Exception*

Executive authority to conduct warrantless electronic surveillance in the name of national security finally met a serious challenge in 1972 when the Supreme Court decided *United States v. United States District Court for the*

---

92. *See* Cinquegrana, *supra* note 33, at 801 ("Congress, like the Supreme Court, was not prepared in 1968 to regulate the executive's claim of inherent power to conduct warrantless electronic surveillance for national security purposes.").

93. 18 U.S.C. § 2511(3) (2000); *see also* Cinquegrana, *supra* note 33, at 801 (noting that Title III "specifically disclaimed any intention that its provisions, or those of the 1934 Communications Act, should be read to affect the constitutional powers of the President to protect the United States against hostile foreign powers, to obtain foreign intelligence information, . . . or to guard against any other 'clear and present danger'").

94. *See* United States v. United States Dist. Ct., 407 U.S. 297, 302-03 (1972) (noting government's reliance on § 2511(3) disclaimer to justify warrantless surveillance of defendants suspected of bombing federal buildings); Cinquegrana, *supra* note 33, at 801 (describing executive branch interpretation of Title III provision as "tacit congressional acceptance" of executive authority to conduct surveillance activities related to national security).

95. *Id.* After the passage of Title III, "it appear[ed] that the only limitations on the President's authority to engage in some forms of electronic surveillance [were] those set forth in the Constitution." United States v. Butenko, 494 F.2d 593, 600 n.25 (3d Cir. 1974) (en banc).

*Eastern District of Michigan*,[96] also known as the *Keith* case.[97] In *Keith*, the Supreme Court considered the Title III national security disclaimer[98] and, for the first time, directly addressed the ultimate question of presidential authority to conduct warrantless surveillance operations in the name of national security.[99] At the outset of his majority opinion, Justice Powell asserted the magnitude and difficulty of the issue before the Court:

> The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. [R]esolution [of the issue] is a matter of national concern, requiring sensitivity both

---

96. 407 U.S. 297 (1972).

97. *See* United States v. U.S. Dist. Ct., 407 U.S. 297, 303 (1972) [hereinafter *Keith*] (holding that Title III was not grant of power to executive in national security cases and that electronic surveillance in domestic security investigation requires prior judicial approval). In *Keith*, the Court directly faced the question of whether the President could "authorize electronic surveillance in internal security matters without prior judicial approval." *Id.* at 299. The Court first examined the procedures for obtaining a warrant for criminal surveillance under Title III. *Id.* at 301-02. In particular, the Court considered language in the statute specifically referring to constitutional authority of the President to protect national security, on which the Government relied to justify its warrantless surveillance. *Id.* at 302. The Court concluded that rather than providing the President with a statutory exemption to the Title III warrant requirement, the language of the statute was merely an effort by Congress to leave "presidential powers where it found them." *Id.* at 303. Thus, the Court reasoned, the executive could not rely on the statute to support the surveillance in question. *Id.* at 308. "Rather, we must look to the constitutional powers of the President." *Id.* Before examining the executive's constitutional power with respect to the instant case, the Court asserted that it did not address "the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* The *Keith* Court noted that the question it addressed was the one left open by Katz: "whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security." *Id.* at 309 (quoting Katz v. United States, 389 U.S. 347, 358 n.23 (1967)). The Court recognized the tremendous interest of the government in national security cases, but asserted that it must balance this interest with the Fourth Amendment's protections. *Id.* at 312-15. The Court concluded that, in the instant case, "the Government's concerns [did] not justify departure . . . from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance." *Id.* at 321. However, before ending its opinion the Court asserted that Congress may prescribe warrant procedures more suited to the requirements of national security than those of Title III that may, if reasonable, comport with the Fourth Amendment. *Id.* at 322-324; *see also* Cinquegrana, *supra* note 33, at 802 ("The seminal case in the development of the law of national security surveillance, however, proved to be the so-called '*Keith*' case . . . .").

98. *Keith*, 407 U.S. at 302-08 (noting Government's reliance on 18 U.S.C. § 2511(3) and considering import of provision).

99. *See id.* at 299 (stating that case "involves the delicate question of the President's power . . . to authorize electronic surveillance in internal security matters without prior judicial approval").

> to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable government intrusion.[100]

In *Keith*, the Government charged the defendants, all of whom were United States citizens, in connection with the bombing of a Central Intelligence Agency (CIA) office in Michigan.[101] The Government's indictment stemmed from evidence obtained through a wiretap authorized by the Attorney General but initiated with no judicial involvement or approval.[102] In defense of the warrantless surveillance, the Government relied on Congress's disclaimer in Title III and asserted that it undertook the surveillance pursuant to the President's constitutional powers to protect national security.[103] Both the district court and the Court of Appeals for the Sixth Circuit disagreed with the Government and held that the surveillance was unlawful under the Fourth Amendment.[104]

In considering the Government's appeal, the Supreme Court looked closely at the overall structure of Title III, but focused particularly on the provision disclaiming any impact on the "constitutional power of the President to take measures" in the interest of national security.[105] This examination led the Court to conclude that the language and history of the legislation did not support the Government's assertion of implicit congressional authority.[106] Instead, the Court interpreted the Title III disclaimer as "Congress simply [leaving] presidential powers where it found them."[107] The Court noted that 18 U.S.C. § 2511(3) did not "employ[ ] the standard language of exception"[108] and cited the legislative history of Title III: "We are not affirmatively conferring any power upon the President. We are simply saying that nothing herein shall limit such power as the President has under the Constitution. We certainly do not grant him a thing."[109] Based on such a clear assertion of congres-

---

100. *Id.*

101. *Id.*

102. *See id.* at 300-01 (describing background of case).

103. *See id.* at 301-02 (noting Government's reliance on § 2511(3) and asserting "that the sureveillance [sic] was lawful, though conducted without prior judicial approval, as a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security").

104. *See id.* at 301 (recounting procedural history of case).

105. 18 U.S.C. § 2511(3); *see Keith*, 407 U.S. at 301-08 (discussing Title III generally and disclaimer in § 2511(3) specifically).

106. *See id.* at 303 (concluding that "the language of § 2511(3), as well as the legislative history of the statute, refutes [the Government's] interpretation").

107. *Id.*

108. *Id.* at 304.

109. *Id.* at 306-07 (emphasis omitted).

sional neutrality, the Court held that the Government could not rely on the Title III disclaimer to support the surveillance at issue.[110]

When the statutory argument failed, the Court next considered whether the Government could rely upon the executive's inherent constitutional powers.[111] The question before the Court was the very one Justice Stewart declined to address in *Katz*: whether prior judicial authorization was a constitutional prerequisite for national security surveillance.[112] Justice Powell's majority opinion recognized that the answer to this question lies in the Fourth Amendment's requirement that all searches be reasonable and "the way in which 'reasonableness' derives content and meaning through reference to the warrant clause."[113]

The Court was quite sensitive to the particularly strong governmental interest in protecting national security[114] and the difficulty of meeting this task in the modern world.[115] On the other hand, the Court noted that "[t]here is, understandably, a deep-seated uneasiness and apprehension that [electronic surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens."[116] The challenge for the Court involved balancing the necessity of ensuring national security against the threat to individual liberties posed by unchecked executive surveillance authority.[117]

In weighing these competing interests, Powell's opinion expanded the principles that would guide all three branches of the federal government in the application of the Fourth Amendment to national security electronic surveillance.[118] Powell noted that national security cases present a particularly

---

110. *See id.* at 308 (holding that Title III "is not the measure of the executive authority asserted in this case").

111. *See id.* (noting that Court must look to constitutional source to derive executive's authority).

112. *See id.* at 309 (noting that *Katz* Court did not answer question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security" (quoting Katz v. United States, 389 U.S. 347, 358 n.23 (1967))).

113. *Id.* at 309-10 (citation omitted).

114. *See id.* at 312 (noting that "unless the Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered").

115. *See id.* at 311-12 (noting that "covertness and complexity of potential unlawful conduct" made electronic surveillance techniques particularly important and that "[i]t would be contrary to the public interest for the Government to deny itself" such tools).

116. *Id.* at 312.

117. *See id.* at 314-15 (noting that Court's "task [was] to examine and balance the basic values at stake in [the] case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression").

118. *See* United States v. Duggan, 743 F.2d 59, 72 (2d Cir. 1984) (noting that decision in

prickly situation because of the tremendous governmental interest[119] and the likelihood of both unreasonable invasions of privacy and jeopardy to free speech rights.[120] Although he recognized the vital importance of protecting the national security, Justice Powell's primary concern was ensuring the sanctity of political dissent – both public and private – in determining the application of the Fourth Amendment to national security surveillance.[121]

For Powell, the Fourth Amendment had to serve as "an important working part of our machinery of government, operating . . . to check the 'well-intentioned but mistakenly over-zealous executive officers.'"[122] This constitutional function could not be guaranteed when domestic security surveillance was left entirely to the discretion of the executive: "*[U]nreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.*"[123] Thus, the Court reiterated its assertion in *Katz* that some interposition of the judiciary between citizens and law enforcement must exist.[124]

The Court noted and carefully considered the Government's argument in favor of a blanket exception to the Fourth Amendment for national security situations.[125] Nevertheless, the majority concluded that "the Government's concerns do not justify departure in this case from the customary Fourth

---

*Keith* "made clear that the requirements of the Fourth Amendment may change" depending on governmental interests and that interests in national security context are "substantially different" from those in criminal investigations).

119. *See Keith*, 407 U.S. at 312 (noting that without national security, all constitutional liberties are at risk).

120. *See id.* at 313 ("National security cases, moreover, 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 a greater jeopardy to constitutionally protected speech.").

121. *See id.* at 314 (discussing political dissent). Justice Powell noted:

> 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.

*Id.*

122. *Id.* at 316 (citation omitted).

123. *Id.* at 316-17 (emphasis added).

124. *See id.* at 317 (noting that while surveillance at issue may have been entirely reasonable, Court had never let this fact excuse lack of judicial involvement prior to surveillance); *id.* at 318 (noting that judicially created exceptions to warrant requirement did not dilute principle of obtaining warrant prior to surveillance whenever practicable).

125. *See id.* at 319-20 (noting pragmatic force of arguments for exception to Fourth Amendment in domestic national security situations).

Amendment requirement of judicial approval prior to initiation of a search or surveillance."[126] However, Powell carefully limited the scope of the opinion as follows:

> We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents. . . . Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to [domestic security] case[s]. . . . Congress may wish to consider protective standards for [such cases] which differ from those already prescribed . . . in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.[127]

Essentially, the Court asserted that legislative action could adapt the Fourth Amendment warrant requirement to the specific needs of the governmental interests in question, *but that any search must be reasonable*.[128]

*Keith* opened the door to modern national security law and Congress eventually accepted the Court's implicit invitation to legislate by enacting FISA.[129] The issue before the Court in *Keith*, however, was surveillance for domestic security operations;[130] the Court explicitly left open an important window for a foreign intelligence exception.[131] Because the Court did not settle the ultimate issue of national security surveillance of an American citizen in a foreign intelligence context, important developments in the lower courts helped to shape FISA.[132] The Supreme Court has never specifically endorsed the existence of a foreign intelligence exception to the Fourth Amendment,[133] but every lower court that has addressed the issue seized upon

---

126. *Id.* at 321.

127. *Id.* at 321-23.

128. *See id.* at 323 ("For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.").

129. *See* Cinquegrana, *supra* note 33, at 802 ("The seminal case in the development of the law of national security surveillance, however, proved to be the so-called '*Keith*' case, *United States v. United States District Court*, decided by the Supreme Court in 1972.").

130. See Keith, 407 U.S. at 299 (noting that surveillance at issue regarded internal security matters).

131. *See id.* at 308 (noting that "the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers").

132. *See* Cinquegrana, *supra* note 33, at 803-04 ("The Supreme Court in *Keith* had not addressed the legality of warrantless electronic surveillance undertaken by the Executive for genuine national security purposes. Lower federal courts, however, continued to grapple with this issue and their opinions also made important contributions to the shaping of FISA.").

133. Reimers, *supra* note 25, at 71.

*Keith*'s disclaimer and endorsed just such an exception.[134] Nevertheless, these courts struggled to reconcile the decision in *Keith* with the Court's other evaluations of the extent of executive prerogative in national security matters.[135]

The most essential development from the cases defining the foreign intelligence exception is the "primary purpose doctrine."[136] The primary purpose doctrine asserts that "prior judicial authorization [is] not required" only when surveillance is "conducted and maintained solely for the purpose of gathering foreign intelligence information."[137] However, review of a warrantless surveillance must affirmatively determine "that [securing foreign intelligence information] was in fact [the search's] primary purpose and that the accumulation of evidence of criminal activity was incidental."[138] Such surveillance still is subject to the reasonableness standard of the Fourth Amendment.[139] The import of this statement is that warrantless electronic surveillance in contravention of the primary purpose doctrine is repugnant to the Fourth Amendment of the Constitution.[140]

*United States v. Truong Dinh Hung*[141] presents a particularly enlightening discussion of the primary purpose doctrine. In *Truong*, the Court of Appeals

---

134. *See* United States v. Duggan, 743 F.2d 59, 72 (2d Cir. 1984) ("Prior to the enactment of FISA, virtually every court that had addressed the issue had concluded that . . . warrantless electronic surveillance to collect foreign intelligence information . . . constituted an exception to the warrant requirement of the Fourth Amendment.").

135. *See United States v. Butenko*, 494 F.2d 593, 602-03 (3d Cir. 1983) (en banc) (discussing *Keith* in relation to other decisions of Court). The Third Circuit noted that:

> The expansive language of United States v. Curtiss-Wright Export Corporation provides support for the contention that the President is authorized to act unencumbered by the Fourth Amendment requirements of prior judicial approval and probable cause when he is dealing with national security matters. The ramifications of *Curtiss-Wright*, however, remain somewhat enigmatic in this regard. To contend that customary Fourth Amendment analysis is to be abandoned whenever the President asserts that a particular search and seizure is incident to the conduct of foreign affairs activities is arguably uncongenial with a reasoned view of the relationship among the relevant constitutional provisions and the thrust of the Supreme Court decision in [*Keith*]. We take no such position here.

*Id.*

136. *See* Reimers, *supra* note 25, at 83 (noting that Court of Appeals for the Third Circuit created national security exception "standard applicable to all U.S. persons which came to be known as the primary purpose doctrine").

137. *Butenko*, 494 F.2d at 605 (internal quotation marks omitted).

138. *Id.* at 606.

139. *See id.* at 605-06 (noting that post-search judicial review often will be necessary to safeguard defendant's Fourth Amendment rights).

140. *See id.* ("The opportunity for post-search judicial review represents an important safeguard of Fourth Amendment rights.").

141. 629 F.2d 908 (4th Cir. 1980).

for the Fourth Circuit struggled with the issue of how to treat evidence obtained in an investigation that served both prosecutorial and intelligence-gathering ends.[142] In so doing, the court recognized the criticality of the purposes of an investigation to the application of the Fourth Amendment.[143] Writing for the majority, Judge Winter espoused the primary purpose doctrine:

> [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 . . . . 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.[144]

Judge Winters noted, however, that a test requiring that surveillance be solely for foreign intelligence purposes was equally unacceptable because many investigations that begin as foreign intelligence culminate in criminal prosecutions.[145]

Thus, although the decision in *Truong* explicitly recognized the existence of the foreign intelligence exception and acknowledged the constraints imposed on the exception by the primary purpose doctrine, it left the parameters of the doctrine ill-defined.[146] Without any clear guidelines as to when

---

142. United States v. Truong Dinh Hung, 629 F.2d 908, 931 (4th Cir. 1980) (holding that warrantless surveillance in espionage case did not violate Fourth Amendment). In *Truong*, the Court of Appeals for the Fourth Circuit considered an appeal from defendants convicted of espionage. *Id.* at 911. Specifically, the court considered the defendants' contention that evidence obtained by warrantless electronic surveillance violated the Fourth Amendment. *Id.* The court disagreed with the defendants' assertion and concluded that "the Executive Branch need not always obtain a warrant for foreign intelligence surveillance." *Id.* at 913. According to the court, the extraordinary interests of the executive in the foreign intelligence realm merited this exception. *Id.* The court went on, however, to carefully limit the exception to surveillance with a direct connection to "a foreign power, its agent or collaborators." *Id.* at 915. "When there is no foreign connection, the Executive's needs become less compelling; and the surveillance more closely resembles the surveillance of suspected criminals, which must be authorized by warrant." *Id.* Thus, the court explicitly endorsed the primary purpose doctrine. *Id.* Because the surveillance at issue met the mandate of the primary purpose doctrine, the Government's evidence was admissible and the court affirmed the defendants' conviction. *Id.* at 931.

143. *See id.* at 915 (noting that "the executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons").

144. *Id.*

145. *See id.* at 915-16 (noting that "there is always the possibility that the targets of the [national security] investigation will be prosecuted for criminal violations").

146. The surveillance at issue in *Truong* occurred before FISA's enactment, but the Fourth

warrantless surveillance was constitutional, the executive faced a difficult choice: it could undertake surveillance without a warrant and jeopardize any subsequent prosecution; or it could seek a traditional warrant and risk the surveillance itself. Rather than solving it, the primary purpose doctrine added yet another dimension to the vexing problem of how to reconcile the necessities of national security surveillance with the Fourth Amendment.

## *III. Modern National Security Surveillance Before September 11th: Fleshing Out FISA*

### *A. The Foreign Intelligence Surveillance Act: Legislative Reconciliation of the Fourth Amendment and National Security Surveillance*

#### *1. Development*

Arguably, one could attribute the same level of ambiguity present in the primary purpose doctrine to the entirety of the judiciary's treatment of national security surveillance. The founding principle asserted in *Katz* – that judicial review for probable cause should precede any surveillance to ensure

---

Circuit did not hand down a decision in the case until after the legislation took effect. *Id.* at 914 n.4. In a footnote, the court remarked upon the statute and offered a fairly in-depth judicial consideration of the new law. *Id.* In the footnote, Judge Winter concluded that although FISA mandated a warrant in some circumstances, it "does not . . . transport the traditional Fourth Amendment warrant requirement unaltered into the foreign intelligence field." *Id.* Furthermore, Judge Winter observed that the warrant procedure under FISA was substantially looser than the requirements for issuing a standard criminal surveillance warrant, noting that for a FISA warrant:

> [T]he executive need demonstrate only . . . that the target is a foreign power or a foreign agent and, in the case of United States citizens and resident aliens, that the government is not clearly erroneous in believing that the information sought is the desired foreign intelligence information and that the information cannot be reasonably obtained by normal methods.

*Id.* (citation omitted). Judge Winter concluded his consideration of FISA by asserting the imprudence of any judicial attempt to impose an "elaborate structure for core foreign intelligence surveillance under the guise of a constitutional decision." *Id.* at 914-15. Despite the reverence to the executive implicit in Judge Winters's footnote, the judge was not willing to ignore completely the danger of allowing government surveillance without prior judicial approval:

> [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 . . . the government should be relieved of seeking a warrant only when the object of the search or the surveillance is a foreign power, its agent or collaborators.

*Id.* at 915.

compliance with the Fourth Amendment's mandate – persisted as the baseline for all inquiry,[147] but the *Katz* Court also made clear that national security surveillance was an unusual creature to which the warrant requirement may not apply.[148] In *Keith*, the Court required the government to obtain judicial authorization before domestic-security surveillance was constitutional, but nevertheless recognized that existing procedures for obtaining judicial authorization may not be appropriate for national security cases.[149] Additionally, in some circumstances, the government may enjoy an exception to the Fourth Amendment's warrant clause altogether.[150] *Truong* seized on *Keith*'s exclusionary possibility to provide judicial support for the executive's ongoing practice of warrantless national security surveillance, but limited the practice with the primary purpose doctrine. This hodgepodge of judicial pronouncements provided all of the pieces for FISA; the only thing absent was impetus.

Ironically, the necessary impetus for FISA's creation grew out of the paradox created by the judiciary's mixed messages. In the mid-1970s it became clear that the executive had chosen to err on the side of breadth in interpreting the foreign intelligence exception to the point of abuse.[151] Reports appeared in the press alleging that the CIA had compiled files on thousands of American citizens.[152] These reports led President Ford and both houses of Congress to form investigative committees to consider the extent of executive surveillance abuses.[153]

---

147. *See supra* notes 72-95 and accompanying text (discussing *Katz* and requirement of judicial authorization for executive surveillance).

148. *See supra* notes 85-88 and accompanying text (discussing footnote 23's exclusion of national security surveillance).

149. *See Keith*, 407 U.S. at 322-23 (suggesting Congress "may wish to consider" different standards for national security surveillance and that such standards "may be compatible with the Fourth Amendment").

150. *See supra* notes 96-128 and accompanying text (discussing *Keith* and possibility of different warrant standards in national security context).

151. *See* Reimers, *supra* note 25, at 63 (discussing executive's abuses of exception). Lt. Reimers notes:

> Congressional involvement . . . remained minimal until the mid-1970s, [when] a series of especially troubling revelations appeared in the press concerning U.S. Intelligence activities. Covert action programs involving assassination attempts against foreign leaders and covert efforts to effect changes in other governments were reported for the first time. The efforts of intelligence agencies to collect information concerning the political activities of U.S. citizens during the late 1960s and early 1970s were also documented extensively by the press.

*Id.* (quoting SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE, 103D CONG., 2ND SESS., REPORT ON LEGISLATIVE OVERSIGHT OF INTELLIGENCE ACTIVITIES: THE U.S. EXPERIENCE 3, 4 (Comm. Print 1994)).

152. *Id.*

153. *See id.* at 64-65 (noting that Ford formed Rockefeller Commission, Senate formed

The findings of these committees were startling. During the 1960s and 1970s, the CIA compiled a computerized database containing thousands of records chronicling the involvement of individual participants in the domestic antiwar movement.[154] From these databases, the CIA "produced a steady stream of reports to the FBI and other agencies detailing the results of its various intelligence activities with respect to the antiwar movement."[155] Between 1967 and 1973, the CIA and other intelligence agencies, as well as the FBI, obtained and compiled the communications of over one thousand United States citizens.[156]

All of this made one fact painfully clear: The "existing legal and policy constraints on intelligence activities were inadequate and . . . proper supervision and accountability within the Executive branch and to the Congress were sorely lacking."[157] Although Title III provided a framework for criminal surveillance, the foreign intelligence exception was the creation of muddled judicial doctrine. Congress recognized that under the then-current system, action by the judiciary was purely remedial, and the courts essentially were powerless to prevent executive abuses before they occurred.[158] Thus, Congress reacted to the executive's abuse of the foreign intelligence exception by creating a system in which "the judiciary would . . . be involved from the onset,"[159] effectively curbing the executive's ability to conduct warrantless national security surveillance that arguably contravened constitutional requirements.[160]

---

Church Committee, and House formed Pike Committee).

154. *See* Halkin v. Helms, 690 F.2d 977, 982 (D.C. Cir. 1982) (describing CIA operation CHAOS and its intelligence gathering methods).

155. *Id.*

156. *See id.* at 983-84 (explaining how agencies gathered this information through National Security Agency's monitoring system).

157. Reimers, *supra* note 25, at 66 (quoting Stephen Saltzburg, *National Security and the Fourth and Fifth Amendments, in* NATIONAL SECURITY LAW 1001, 1008 (John Norton Moore et al. eds., 1990)).

158. *See id.* at 74 (noting that Congress was aware of "case law imposing the Fourth Amendment on the executive branch" and knew that "courts did not get an intelligence case until after an abuse occurred").

159. *Id.*; *see also In re* Kevork, 788 F.2d 566, 569 (9th Cir. 1986) (noting that enactment of FISA sought to balance need for adequate foreign intelligence surveillance procedures with protection of civil liberties); Reimers, *supra* note 25, at 62 (noting that FISA was "the Congressional reaction to executive branch violations of basic American civil liberties under the guise of the so called 'national security exception' to the Fourth Amendment").

160. *See id.* at 71 (noting "the enactment of FISA . . . curtailed the Executive Branch's ability to conduct warrantless electronic surveillance").

### *2. Structure and Procedures*

FISA did for foreign intelligence operations what Title III had done for traditional criminal investigations. Specifically, it "creat[ed] a secure framework by which the executive branch [could] conduct legitimate electronic surveillance for foreign intelligence purposes within the context of [the United States'] commitment to privacy and individual rights."[161] This framework imposed several procedural hurdles for executive agents seeking surveillance authorization under the Act.

FISA incorporates the first principle of constitutional surveillance – prior judicial authorization – in most circumstances,[162] but the initial steps in the procedure occur entirely within the executive branch. To obtain FISA authorization, an investigating agent must first submit an application to the Office of Intelligence Policy and Review (OIPR), an internal branch of DOJ, which makes an initial determination of whether sufficient evidence exists to demonstrate probable cause for electronic surveillance under FISA.[163] If the OIPR finds that the application presents sufficient evidence, the office submits the application to the Attorney General for a second review.[164] If the Attorney General agrees with the OIPR that there is sufficient evidence for probable cause, then the Attorney General must give the application official personal approval before forwarding the matter to the Foreign Intelligence Surveillance Court (FISC) for final approval and authorization.[165]

Although FISA acknowledges the foreign intelligence exception and allows warrantless surveillance in certain very limited circumstances,[166] the FISC considers the majority of executive requests for surveillance authorization under the Act.[167] Applications to the FISC must meet three primary substantive requirements. First, the application must contain a statement of

---

161. United States v. Pelton, 835 F.2d 1067, 1074 (4th Cir. 1987) (citation and internal quotation marks omitted).

162. *See* 50 U.S.C. § 1804 (1994) (requiring submission of FISA applications to federal judge).

163. *See* Reimers, *supra* note 25, at 57 (stating that review by OIPR is first step in FISA authorization).

164. *See id.* (describing next step in FISA authorization).

165. *See id.* (explaining steps in obtaining FISA authorization); *see also* 50 U.S.C. § 1804(b) (1994) (same).

166. *See* 50 U.S.C. § 1802(a) (1994) (noting that Attorney General may authorize warrantless surveillance for up to one year by certifying under oath that surveillance at issue meets specific requirements); *id.* § 1811 (authorizing warrantless surveillance for fifteen days following declaration of war).

167. *See id.* § 1804(a) (noting that all FISA applications for electronic surveillance "shall be made by a federal officer in writing upon oath or affirmation to a [FISA] judge").

reasons to believe that "the target of the surveillance is a foreign power or an agent of a foreign power."[168] Second, the application must contain information on the manner of conduct of the surveillance, including the identity of the target if known and proposed minimization procedures.[169] Finally, a high-ranking executive branch official must certify the application and state that he "deems the information sought to be foreign intelligence information" and that the government cannot obtain the information sought by other means.[170]

Several factors make the FISC's review much less stringent than Title III review and, thus, less of a safeguard for civil liberties. First and foremost, the standard for probable cause under FISA is lower than that under Title III.[171] Prior to PATRIOT, FISA applications only had to show facts sufficient to justify a belief that the target of the surveillance is a "foreign power or an agent of a foreign power," that "the purpose of the surveillance is to obtain foreign intelligence information," and that the information is unobtainable without a FISA warrant.[172]

FISA's justification-of-belief standard contrasts sharply with Title III, which grants a warrant only when "there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense."[173] At least one commentator has argued that the multi-step progression required to obtain a warrant under FISA actually is a more stringent process than the process under Title III.[174] However, this is not the majority view;[175] the consensus opinion seems to be that "prerequisites to [FISA]

---

168. *Id.*

169. *Id.*

170. *Id.*

171. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915 n.4 (4th Cir. 1980) (noting that FISA "does not require the executive to satisfy the usual standards for the issuance of a warrant"); Sievert, *supra* note 16, at 1437 (noting that probable cause under FISA "contrasts dramatically with Title III").

172. 50 U.S.C. § 1804 (1994).

173. *Id.* § 2518(3).

174. *See* Cinquegrana, *supra* note 33, at 815 (noting that proponents of FISA assert that executive branch exercises careful judgment in initial reviews to insure applications meet proper standards before presentation to FISC); Reimers, *supra* note 25, at 85 (asserting that probable cause standard under FISA "is far more demanding than the criminal standard for U.S. person targets").

175. *See* United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (noting that FISA judge need find only that target is agent of foreign power); United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) (noting that "prerequisites to [FISA] surveillance . . . are less stringent than those precedent to the issuance of a [criminal] warrant"); *Truong*, 629 F.2d at 915 n.4 (noting that FISA does not "require the executive to satisfy the usual standards for the issuance of a warrant"); *Protecting Constitutional Freedoms, supra* note 36 (statement of Douglas W. Kmiec, Dean of the Law School, Catholic University of America) (noting that FISA application

surveillance . . . are less stringent than those precedent to the issuance of a [criminal] warrant."[176]

The second factor that makes FISA a more lenient hurdle is the fact that the executive has the sole power to make the initial – and most important – probable cause determination in the FISA process. Although the FISC makes the final determination of probable cause as defined by FISA, this is an undeniably limited role.[177] The reviewing FISC judge ascertains only whether the executive's certification that the government is undertaking the surveillance to obtain foreign intelligence information is "clearly erroneous."[178] Once the Attorney General certifies that the surveillance seeks foreign intelligence information, it is presumed that the representations made in support of the certification are valid[179] and the application is "subjected to only minimal scrutiny by the courts."[180] Thus, although the probable cause verification is nominally a judicial responsibility, the executive has sole authority to make the substantive determination and the FISC is obliged to accept it.[181] This clearly relaxes the level of scrutiny applied in the probable cause determination as compared to review under Title III. In addition, this procedure arguably eviscerates any purported adherence to the first guiding principle for surveillance – that there be a judicial officer interposed between citizens and the police.[182]

The final aspect of FISA that makes it at once so appealing to prosecutors and so troublesome to civil libertarians is the secrecy which inheres in the process.[183] It hardly is surprising that FISA procedures often are intentionally

---

must show that "information sought is foreign intelligence information," but that "as against foreign powers or agents thereof," it need not demonstrate probable cause). The plain language of the two statutes controverts the assertion that FISA is more stringent. Title III requires that a crime is being, has been, or is about to be committed and that evidence of this criminal activity likely will be obtained. 18 U.S.C. § 2518(3) (1994). FISA, on the other hand, only requires a showing that a crime may be committed and that the surveillance seeks foreign intelligence information. *See* Cinquegrana, *supra* note 33, at 816 (noting FISA standard that crime "may be" committed).

176. United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984).

177. *See id.* at 75 (noting that FISC is not "to make findings" on whether government undertakes surveillance to obtain foreign intelligence information).

178. *Id.* (citing 18 U.S.C. § 1805(a)(5) (1994)).

179. *See id.* at 77 n.6 (noting that "representations and certifications submitted in support of an application for FISA surveillance should be presumed valid").

180. *Id.* at 77.

181. *See id.* (noting that neither FISC nor any court entertaining challenge to FISA surveillance has "authority to second-guess the executive branch's certifications").

182. *See supra* notes 80-84 and accompanying text (noting Supreme Court's refusal to validate governmental surveillance *post facto*).

183. *See* Marrera v. U.S. Dept. of Justice, 622 F. Supp. 51, 53 (D.D.C. 1985) (noting

concealed considering the clandestine nature of counterintelligence operations.[184] However, FISA detractors "argue that the secrecy that surrounds the FISC prevents a determination of whether . . . the FISC has become a captive of the national security establishment and serves only to encourage executive officials, now protected by judicial approval, to conduct activities that would otherwise never have been proposed."[185] This argument derives considerable weight from the fact that in the first ten years of FISA's existence, the FISC denied none of the more than 4,000 applications and that by the year 2000, the court had approved over 11,000 applications.[186]

FISA's secrecy also presents a unique problem for a criminal defendant seeking to suppress FISA surveillance evidence or challenge a conviction based on such evidence. Section 1806(f) of the Act requires that the district court judge entertaining a defendant's challenge to a FISA application "review in camera and ex parte the application, order, and such other [necessary] materials relating to the surveillance" whenever "the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States."[187] Thus, FISA often will not allow a defendant the opportunity to contest adequately the validity of surveillance or the admissibility of crucial evidence obtained thereby. Although courts have affirmed the constitutionality of this reality,[188] the provision nevertheless augments the possibility that governmental abuse of FISA will go undiscovered.

### 3. *FISA Under Fire: Challenges to the Foreign Intelligence Surveillance Act*

Not surprisingly, in light of the preceding discussion, FISA has endured repeated challenges throughout its existence, many founded on issues consid-

---

Freedom of Information Exemption available for FISA materials that "[are] specifically authorized to be kept secret in the interests of national security"); *see also* 50 U.S.C. § 1805(a) (1994) (noting that FISA surveillance orders are to be ex parte); *id.* § 1806(f) (requiring judge reviewing challenge to FISA surveillance to hold hearing in camera and ex parte upon request of Attorney General).

184. *See* Reimers, *supra* note 25, at 59 (noting that once investigation is made public "[a]ny further pursuit of a FISA warrant . . . would [defeat the investigation's] purpose. The cat [would be] out of the bag.").

185. Cinquegrana, *supra* note 33, at 815.

186. *See* Reimers, *supra* note 25, at 91 (noting that "in the last 20 years, over 11,000 wiretaps or search warrants were approved by the FISA court").

187. 50 U.S.C. § 1806(f) (2001).

188. *See* United States v. Belfield, 692 F.2d 141, 148-49 (D.C. Cir. 1982) (finding that 50 U.S.C. § 1806(f) does not violate Fifth and Sixth Amendments).

ered by Congress before enactment.[189] However, just as they endorsed the existence of a foreign intelligence exception to the Fourth Amendment,[190] lower federal courts consistently have upheld FISA against myriad constitutional attacks.[191] The most important challenges to FISA's validity for purposes of this Note are: (1) those asserting that judicially authorized surveillance in the absence of probable cause that a crime is being, has been, or is about to be committed is unconstitutional under the Fourth Amendment;[192] and (2) those disputing the efficacy of FISA's implementation by the executive and FISC.[193]

The Court of Appeals for the Second Circuit's decision in *United States v. Duggan*[194] effectively illustrates the federal judiciary's treatment of these arguments.[195] In *Duggan*,[196] most of the defendants – alleged agents of the

---

189. *See* Cinquegrana, *supra* note 33, at 816 (noting constitutional issues "debated during consideration of the various bills that preceded the enactment of FISA have persisted").

190. *See* United States v. Duggan, 743 F.2d 59, 72 (2d Cir. 1984) (noting that "[p]rior to the enactment of FISA, virtually every court that had addressed the issue had concluded that the President had the inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment").

191. *See* Reimers, *supra* note 25, at 77 (noting that "federal courts have upheld FISA's constitutionality from just about every angle of attack").

192. *See* Cinquegrana, *supra* note 33, at 816 (noting continued "concern over whether surveillance should be authorized" without traditional probable cause determination).

193. *See id.* at 816-17 (noting that "faithfulness of FISA implementation by the Executive and the FISC . . . has undergone repeated scrutiny by the federal courts").

194. 743 F.2d 59 (2d Cir. 1984).

195. *See* Cinquegrana, *supra* note 33, at 817 (noting that opinion in *Duggan* best illustrates "arguments challenging the structure and implementation of FISA" and judicial response to them).

196. *See* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984) (holding FISA constitutional and finding evidence obtained incident to FISA surveillance admissible). In *Duggan*, the Court of Appeals for the Second Circuit addressed the constitutionality and appropriate application of FISA in the context of an investigation of alleged members of the Provisional Irish Republican Army (PIRA). *Id.* at 64. The defendants in *Duggan* appealed their convictions for various firearms-related offenses on the grounds that, *inter alia*, the court should not have admitted the FISA evidence that the Government relied upon to obtain the convictions. *Id.* at 64-65. The defendants asserted that FISA violated the Fourth Amendment, that it was overly broad, and that the Government improperly applied it. *Id.* at 65. After reviewing the structure of FISA, the Second Circuit rejected each of the defendants' arguments. *Id.* at 69-74. In particular, the court noted the existence of a foreign intelligence exception before the enactment of FISA and the Supreme Court's implicit authorization of a different probable cause standard for national security cases such as *Keith*. *Id.* at 72-73. Thus, the court rejected the defendants' constitutional arguments. *Id.* As to the allegedly improper implementation of FISA, the court acknowledged the incorporation of the primary purpose doctrine, but concluded that evidence obtained pursuant to a proper FISA warrant was admissible in a criminal trial. *Id.* at 77. Thus,

Provisional Irish Republican Army (PIRA) – were illegal aliens; Duggan, however, was a United States citizen.[197] Pursuant to a FISA warrant, the government intercepted communications between Duggan and his co-conspirators and videotaped Duggan's negotiations with a FBI agent who posed as an arms dealer.[198] The evidence thus obtained proved critical to the Government's case against Duggan and the other PIRA members.[199]

Pretrial, the defendants sought a hearing to suppress the FISA evidence on the grounds, *inter alia*, that the Government improperly used FISA to obtain evidence for a criminal prosecution, and that, in any event, the surveillance was unconstitutional under the Fourth Amendment.[200] In response, the acting Attorney General moved to have the issue heard in camera because "disclosure or an adversary hearing with respect to [the surveillance] information would harm the national security of the United States."[201] The trial court granted the Government's request and subsequently dismissed all of the defendants' FISA arguments.[202] The defendants, undeterred, persisted in their challenge to the Government's evidence post-trial on the grounds that the Government did not name Duggan as a target in the surveillance application as required under FISA.[203] The court rejected this argument as well.[204] The court ultimately convicted Duggan and the rest of the defendants on various firearms offenses.[205]

On appeal, the defendants renewed their challenges to the constitutionality of FISA and its application in their case, providing the Second Circuit with a prime opportunity to expound upon the Act.[206] The defendants' first constitutional challenge centered on their assertion that FISA's structure was overly broad. They alleged that the definitions of "foreign intelligence information" and "agent of a foreign power" give "the Act unlimited scope and [permit] the electronic surveillance of persons who 'may' be engaging in activities that

---

the court upheld the defendants' convictions. *Id.* at 85.

197. *See id* at 64-65 (discussing background of case).

198. *See id.* at 66 (describing means by which Government obtained evidence).

199. *See id.* at 65 (listing types of evidence used at trial).

200. *See id.* at 67 (noting defendants' contention that FISA surveillance was unconstitutional and "that FISA had been improperly used simply to obtain evidence of criminal activity rather than to protect the national security").

201. *Id.*

202. *Id.*

203. *See id.* at 68 (discussing defendants' post-trial FISA motion).

204. *Id.*

205. *See id.* at 64 (listing defendants' convictions).

206. *See id.* at 64-65 (describing issues on appeal).

'may' violate United States law."[207] The court noted the theoretical appeal of the defendants' arguments, but concluded that their challenge to the scope of FISA had no application to the case before the court.[208] Importantly, however, the court asserted in dicta that it did not find FISA's concepts overly vague, implicitly endorsing the structure Congress provided for national security cases.[209]

The court then turned to the defendants' Fourth Amendment challenge.[210] The court initially noted that prior to FISA there was general acceptance of a foreign intelligence exception to the Fourth Amendment, grounded in the executive's inherent authority under the Constitution, but that the Supreme Court never had directly addressed the issue. [211] However, the court did find support for FISA's procedures in *Keith*. The majority opinion in *Keith* asserted that the Fourth Amendment's application to the realm of foreign intelligence may differ from its application in the context of criminal investigations.[212] Ultimately, the court found that FISA did not violate the Fourth Amendment:

> We regard the procedures fashioned in FISA as a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information. The governmental concerns . . . make reasonable the adoption of prerequisites to surveillance that are less stringent than those precedent to the issuance of a warrant for a criminal investigation. . . . We conclude that [FISA's] requirements provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information, and that FISA does not violate the probable cause requirement of the Fourth Amendment.[213]

---

207. *Id.* at 71.

208. *See id.* ("Interesting though these arguments may be in the abstract, they have no application to the case at hand. . . . The sections of the Act relied upon by the defendants to show that the Act is impermissibly broad are simply irrelevant to this case.").

209. *See id.* (stating that "even if we thought [the specified section of FISA's] concepts of national defense, national security, or conduct of foreign affairs to be vague, which we do not," court nevertheless would refuse to reverse defendants' convictions because they did not result from that section of FISA).

210. *Id.* at 72.

211. *See id.* (discussing history of Fourth Amendment challenges to executive surveillance power).

212. *See id.* (noting that *Keith* "declined to address [the] issue," but "made [it] clear that the requirements of the Fourth Amendment may change when differing governmental interests are at stake and . . . that the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations" (citations omitted)).

213. *Id.* at 73-74.

Finally, the court turned to the defendants' assertion that the FISA surveillance in the instant case was improper because the Government had sought it "as part of a criminal investigation."[214] The court confirmed that FISA surveillance primarily must seek to obtain foreign intelligence, but nevertheless rejected the defendants' argument.[215] After reviewing the FISA application in camera, the court concluded that the Government had met FISA's requirements throughout the conduct of the surveillance.[216]

The court went on to "emphasize that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used . . . as evidence in a criminal trial."[217] The effect of this portion of the court's opinion – just as it had been in the context of the foreign intelligence exception – was to leave the primary purpose doctrine as incorporated into FISA with no clear boundaries. This fact makes evaluation of the constitutionality of PATRIOT's changes to FISA with respect to the purpose of surveillance operations particularly troubling.[218]

### *B. Building the Wall: Separating the Intelligence and Law Enforcement Communities*

#### *1. History, Development, and Incorporation into Foreign Intelligence Surveillance Act*

The historic rift between executive agencies charged with law enforcement and those assigned intelligence duties is due in part to the reality that the two groups traditionally have performed very different duties.[219] However, it also has deep statutory roots. Congress implicitly endorsed separation in its "first lunge into the Executive's realm of foreign intelligence," in the 1947 National Security Act.[220] The National Security Act created the CIA and granted it broad powers.[221] Concurrently, however, the Act specifically for-

---

214. *Id.* at 77.

215. *See id.* (reiterating FISA certification process and limited judicial scrutiny).

216. *See id.* at 78 (affirming district court's finding that surveillance had proper motivation).

217. *Id.*

218. Without a clear judicial pronouncement as to when foreign intelligence is not "the purpose" of FISA surveillance, it is exceedingly difficult to determine how much leeway a court will afford the executive when it asserts that foreign intelligence was a "substantial purpose" of FISA surveillance.

219. *See* Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331, 337 (1998) (noting that "each set of organizations is created and operated with certain clear responsibilities").

220. 50 U.S.C. §§ 401-41 (1994).

221. *See* Reimers, *supra* note 25, at 73 (noting that National Security Act created CIA).

bade the agency from exercising "police, subpoena, law-enforcement powers, or internal-security functions."[222] One court espoused that the National Security Act embodied "Congress'[s] firm resolve to insure that the CIA's 'power that flows from money and stealth' could not be turned loose in domestic investigations of Americans."[223] It was a reflection of "Congress's realistic fear of a secret police, and its desire to protect America's security without 'making the mistake of creating an American Gestapo.'"[224]

The demarcation of duties set forth in the National Security Act persisted through the second half of the twentieth century.[225] However, during much of this time, Congress largely disregarded executive surveillance efforts[226] and was oblivious to ongoing executive surveillance mischief.[227] When these widespread abuses "in the area[s] of intelligence and national security-related activities" finally found their way into the congressional consciousness, they created an "antagonism toward the Executive" that reinforced the sentiment that intelligence gathering operations should remain entirely separate from law enforcement operations.[228] Thus, when Congress sought to structure executive national security surveillance in FISA, it was keenly aware that the new Act held the potential for abuse, and it incorporated the doctrine of separation into the statute.[229]

### *2. Modern Realities Blurring the Line*

As the preceding section noted, a primary reason for the historic division of law enforcement operations and intelligence gathering activities was the

---

222. 50 U.S.C. § 403-3(d) (1994).

223. Marks v. Central Intelligence Agency, 590 F.2d 997, 1007-08 (D.C. Cir. 1978) (Wright, J. dissenting) (citations omitted).

224. *Id.* at 1001 (citation and internal quotation marks omitted).

225. *See* Fredman, *supra* note 219, at 335 (noting clear division between work of intelligence and law enforcement communities during Cold War).

226. *See supra* notes 92-95 and accompanying text (discussing Title III's specific exemption of national security related matters).

227. *See* Reimers, *supra* note 25, at 73 (noting that Congress trusted system created by National Security Act, while executive intelligence agencies engaged in many questionable warrantless surveillance activities).

228. Cinquegrana, *supra* note 33, at 806.

229. *See* 18 U.S.C. § 1806(b)-(d) (2001) (limiting availability of information acquired by FISA for criminal prosecutions); *id.* § 1806(k) (delineating authority to cooperate with law enforcement); *see also Protecting Constitutional Freedoms*, *supra* note 36 (statement of Jerry Berman, Executive Director, Center for Democracy & Technology) (noting that Congress "demanded that the powers bestowed by FISA be strongly contained, and that a clear separation – a wall – be erected between the unique and broad standards for surveillance described in FISA, and those used in the rest of the criminal justice system").

different roles these organizations played within the federal government. This justification worked well in 1947, when there was very little overlap in the communities' respective roles.[230] However, modern crimes such as international terrorism and narcotics trafficking impose a challenge that has been the catalyst for an "erosion of the jurisdictional firewall traditionally dividing domestic law enforcement agencies from the intelligence community in the United States."[231] In these areas, it is no longer clear which agency should take the reins, and the traditional and statutory division has become less tenable.[232]

Notwithstanding the jurisdictional blurring, intelligence and law enforcement communities still operate in paradigmatically different ways to accommodate their respective responsibilities.[233] The primary goal for law enforcement agencies is the conviction of criminals.[234] This function requires that law enforcement act within "precise constitutional and statutory requirements" to ensure that evidence obtained in the course of a particular investigation is admissible in a subsequent prosecution.[235] Furthermore, the investigative sources supporting criminal prosecutions generally must be demonstrable and available for challenge by defense counsel.[236] Intelligence agencies, on the other hand, operate pursuant to an entirely different legal structure based on entirely different authority.[237] Many of the sources upon which the CIA, the National Security Agency, and other executive intelligence organizations rely cannot, by their nature, be exposed in court without jeopardizing ongoing operations, active agents, and sensitive national security information.[238]

The confluence of substantial overlap between intelligence and law enforcement targets and persistently divergent *modus operandi* gives rise to significant procedural and evidentiary problems.[239] Specifically, law enforce-

---

230. *See* Fredman, *supra* note 219, at 335 (noting that there was little overlap between intelligence activities and law enforcement in 1947).

231. *Id.* at 331.

232. *See id.* at 336 (noting that "there is no clear primacy for either the law enforcement or intelligence communities in the realms of international terrorism [and] narcotics").

233. *See id.* at 336-37 (noting that "law enforcement and intelligence communities remain designed and operated in fundamentally dissimilar manners" to meet "certain clear responsibilities").

234. *See id.* (discussing basic operation of law enforcement agencies).

235. *Id.*

236. *See id.* (describing practices of law enforcement agencies).

237. *See id.* (providing basic operation of intelligence agencies as contrast).

238. *See id.* (noting that "intelligence agencies normally depend on sources that cannot be revealed in court").

239. *See id.* (presenting interesting discussion of criminal procedure issues arising out of increasing overlap of law enforcement and intelligence operations).

ment's reliance on evidence obtained by intelligence agencies may "jeopardize the specific legal authority of those intelligence agencies to collect information . . . and also could raise a question of compliance by the CIA with the law enforcement proviso of the National Security Act."[240] Undoubtedly these problems will only become more pervasive as terrorism becomes the chief threat to United States security. It remains to be seen, however, whether Congress's statutory blurring of the jurisdictional lines in PATRIOT will provide a remedy, complicate matters further, or create heretofore unforeseen problems.

### *IV. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*

> Many of the choices that we will face after September 11 will test both our ideals and our resolve to defend them. And as these choices emerge, let us first pause long enough to ask, "What does it gain us?"[241]

The preceding Parts of this Note discuss the arduous task that both the federal judiciary and Congress face whenever they seek to balance national security interests against civil liberties concerns and construct a workable, constitutional system of regulation for executive surveillance. PATRIOT represents the latest effort at striking this balance and seeks to enable law enforcement to meet emerging terrorist threats without curtailing Americans' constitutional rights. It would be extremely naïve, then, to assume that this twenty-first century legislation will be immune from the difficulties that arose for the laws born of the twentieth century.

PATRIOT effects sweeping changes in the way the federal government conducts national security investigations.[242] Only time will tell what success these changes will have in preventing further terrorist acts. Similarly, one cannot know now what impact PATRIOT will have on civil liberties. However, the depth of the changes to the existing structure of foreign intelligence gathering all but ensures new Fourth Amendment dilemmas.[243] This, combined with the fact that Congress drafted and enacted PATRIOT in what may be the most trying time our nation ever has endured, makes it critically important that scholars and citizens carefully examine the provisions of the Act against the lessons of history. In particular, two sections of PATRIOT merit close attention and evaluation under Fourth Amendment principles: the provisions

---

240. *Id.* at 331.

241. *Preserving Freedoms*, *supra* note 35 (statement of Sen. Patrick Leahy).

242. *See infra* Part IV.A (discussing PATRIOT and changes it brings to FISA).

243. *See infra* Part IV.A (discussing PATRIOT and changes it brings to FISA).

allowing increased access to the relaxed standards of FISA, and those facilitating the dissemination of FISA information between the law enforcement and intelligence communities.[244]

### A. Specific Provisions

Several of PATRIOT's provisions increase the government's authority and ability to monitor wire and electronic communication.[245] This new authority, coupled with the incredible technology available to law enforcement, makes the capacity of government surveillance staggering.[246] As the administration began to push for new surveillance powers in the aftermath of 9-11, civil libertarians and national security experts began to question whether the increased authority was the right solution because the executive "already possess[ed] immense statutory power to act on [its] own without Congress or extensive judicial involvement."[247]

Some experts have suggested, perhaps cynically, that certain persons forced PATRIOT through Congress to "maintain public support or to insulate anticipated criminal prosecutions from constitutional challenges."[248] The latter contention is quite tenable in light of the fact that the Supreme Court has not yet addressed the constitutionality of FISA surveillance.[249] In considering the changes PATRIOT brings to FISA and assessing the constitutionality of the new laws as written, it is imperative to remember the possible motives

---

244. *See infra* Part IV.A (discussing PATRIOT and changes it brings to FISA).

245. *See* PATRIOT, *supra* note 18, § 201, 115 Stat. at 278 (adding terrorism offenses to predicate offenses for which Title III orders are available); *id.* § 206, 115 Stat. at 282 (authorizing roving wiretap surveillance pursuant to FISA warrant); *id.* § 209, 115 Stat. at 286-87 (allowing seizure of voice mail pursuant to search warrant rather than wiretap order); *id.* § 214, 115 Stat. at 286-87 (extending pen register/trap and trace authority to FISA); *id.* § 219, 115 Stat. at 291 (allowing issuance of nationwide surveillance warrants in terrorism investigations); *id.* § 503, 115 Stat. at 364 (expanding DNA sample collection predicates to include all crimes of violence as well as attempts and conspiracies to commit such crimes); *id.* § 507, 115 Stat. at 367-68 (authorizing ex parte orders to obtain education records in investigations of international or domestic terrorism).

246. *See* Young, *supra* note 25, at 1066 (noting government's access to "powerful technologies for surveillance and monitoring of citizens" and that "technological advances will continue to augment these substantial capabilities"); *id.* at 1070-71 (noting that combination of surveillance technology and computer processing capabilities allows government to "monitor its citizens . . . more efficiently and more effectively").

247. *Wider Surveillance Powers Urged, But Some Already Available*, ABA JOURNAL EREPORT, Sept. 21, 2001, *at* http://www.abanet.org/journal/ereport/civil.html (last visited Sept. 23, 2001).

248. *Id.*

249. *See id.* (noting that "Supreme Court never has confronted the constitutionality of FISA").

underlying the Act's creation. Furthermore, it is particularly important to address the manner in which agencies ultimately will use the new laws.

### *1. Section 218: Lowering the Threshold for Obtaining FISA Authorization*

The single most important provision in PATRIOT for purposes of this Note seems quite trivial on its face: Section 218 of PATRIOT amends Section 303(a)(7)(B) of FISA by striking "*the* purpose" and inserting "*a significant* purpose."[250] This means that although the Attorney General originally had to certify that "the purpose of the surveillance [was] to obtain foreign intelligence information" in order to obtain FISA authorization, he now need only certify that foreign intelligence is a "significant purpose" of the surveillance.[251] The textual modification to FISA is negligible, but the impact of the change is potentially massive.

A testament to the significance of this seemingly inconsequential change is the amount of congressional testimony and deliberation § 218 drew during the consideration of PATRIOT.[252] Senator Feingold summarized the prevailing concern expressed by PATRIOT's detractors as follows:

> I am also very troubled by the broad expansion of Government power under . . . FISA. When Congress passed FISA in 1978, it granted to the executive branch the power to conduct surveillance in foreign intelligence investigations without having to meet the rigorous probable cause standard under the [F]ourth [A]mendment that is required for criminal investigations. There is a lower threshold for obtaining a wiretap order from the FISA court because the FBI is not investigating a crime, it is investigating foreign intelligence activities. But the law [before PATRIOT] requires that intelligence gathering be the primary purpose of the investigation in order for this much lower standard to apply. [PATRIOT] changes that requirement.[253]

Simply put, this change to FISA eviscerates the end result of years of judicial and congressional efforts to delineate how the government may conduct national security surveillance under the Constitution.

The implications of § 218 are particularly clear when considered against the judiciary's consistent reliance on the primary purpose doctrine in reconciling the foreign intelligence exception with the Fourth Amendment, and Con-

---

250. PATRIOT, *supra* note 18, § 218, 115 Stat. at 291 (emphasis added).

251. 50 U.S.C. § 1804(a)(7) (2001).

252. *See Constitutionality of Various Provisions of the Proposed Anti-Terrorism Act of 2001: Hearing Before the Senate Judiciary Comm.*, 107th Cong. (2001) (statement of Douglas W. Kmiec, Dean of the Law School, Catholic University of America) (noting that "a good deal of debate has focused" on change to FISA).

253. 147 CONG. REC. S11,021 (2001) (statement of Sen. Feingold).

gress's inclusion of the doctrine in the original structure of FISA.[254] PATRIOT excises the primary purpose doctrine from the structure of FISA and substitutes an entirely new paradigm, which this Note calls the substantial purpose doctrine. The net effect of this new doctrine is that overzealous prosecutors now can invoke the skeleton key of terrorism in what might otherwise be garden-variety criminal investigations, and open the door to the less stringent judicial review of the FISC.[255] Arguably, the primary purpose doctrine is essential to the constitutionality of both the pre-FISA foreign intelligence exception and FISA itself. It remains to be seen whether either can survive a Fourth Amendment challenge without it.

The ease with which numerous entities already have used the fear of terrorism to achieve their own ends makes the increased access to FISA warrants particularly troubling.[256] As Senator Feingold recognized during consideration of PATRIOT, "[i]t seems obvious that with this lower standard, the FBI will . . . try to use FISA as much as it can."[257] This, Senator Feingold continued, often could abridge Fourth Amendment rights in terrorist investigations.[258] This is not particularly troubling in the foreign terrorism context

---

254. *See supra* notes 136-46 and accompanying text (discussing primary purpose doctrine).

255. *See* 147 CONG. REC. S11,021-22 (2001) (statement of Sen. Feingold) (noting that "FBI will . . . try to use FISA as much as it can"); WHITEHEAD & ADEN, *supra* note 30, at 26 (noting that provision expands access to FISA's "looser standards").

256. Not surprisingly, one of the first examples of opportunistic use of America's new fear of terrorism is lobbying efforts on Capitol Hill. Advocacy groups have recast their existing goals in terms of bolstering homeland defense, hoping to secure funds already earmarked for the war on terror. David E. Rosenbaum, *Since September 11, Lobbyists Use New Pitches for Old Pleas*, N.Y. TIMES ONLINE, Dec. 3, 2001, *at* http://www.nytimes.com/2001/12/03/politics/03LOBB.html (last visited Jan. 25, 2002). Observers also have drawn analogies between terrorism and the actions of the leaders of Enron, the energy giant that declared bankruptcy amid allegations of a spectacular accounting scandal. *See Review and Outlook: The Federal Enron*, WALL ST. J., Feb. 14, 2002, at A20 (noting that "members of Congress are having a gay old time accusing Enron executives of 'economic terrorism'"). More importantly for this Note, some observers have already labeled the war on drugs an indirect war on terrorism. *See infra* notes 292-98 and accompanying text (discussing potential for expansion of PATRIOT's tools to fight war on drugs).

257. 147 CONG. REC. S11,021-22 (2001) (statement of Sen. Feingold).

258. *See* 147 CONG. REC. S11,022 (2001) (statement of Sen. Feingold) (discussing possibility of abuse of Fourth Amendment rights in terrorism investigations). Senator Feingold stated:

> It seems obvious that with this lower standard, the FBI will . . . try to use FISA as much as it can. And, of course, with terrorism investigations, that won't be difficult because the terrorists are apparently sponsored or at least supported by foreign governments. So this means the [F]ourth [A]mendment rights will be significantly curtailed in many investigations of terrorist acts.

147 CONG. REC. S11,022 (2001) (statement of Sen. Feingold).

because even entirely warrantless surveillance may still enjoy judicial exemption from the Fourth Amendment via the foreign intelligence exception. However, if the executive should implement PATRIOT for surveillance outside of that context – for example, in a domestic terrorism investigation – the revised FISA procedures may be inadequate to ensure that a search is constitutionally reasonable.

The new relaxed standards that PATRIOT brings to FISA raises yet another question: Why did the executive feel that it needed the lower standard? In its twenty-four-year history, the FISC has not "denied a single one of more than 10,000 applications."[259] One could argue that the tragedy of 9-11 led the executive rashly to seek an expansion of FISA's jurisdictional breadth. Although this expansion may enhance the United States' ability to defend against terrorism, it concurrently increases the likelihood that executive agencies will abuse FISA. Thus, PATRIOT circumvents FISA's original intent: curbing executive abuse of the foreign intelligence exception.

### 2. *Section 203: Sharing of Information Between Law Enforcement and Intelligence Agencies*

The fact that PATRIOT allows broad dissemination of information obtained by FISA surveillance compounds the danger of granting executive agencies increased access to FISA. Section 203(b) of PATRIOT amends the criminal code to allow:

> any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence information . . . to assist the official who is to receive that information in the performance of his official duties.[260]

Section 203 goes on to provide two new definitions of foreign intelligence information. The first definition is fairly concise but still leaves room for interpretation, encompassing information relating to the United States' ability to protect against: (1) attack by a foreign power or its agent, (2) sabotage or terrorism by a foreign power or its agent, or (3) espionage by a foreign power or its agent.[261] The second classification is much broader, defining information

---

259. Philip Shenon, *Paper Court Comes to Life Over Secret Tribunal's Ruling on Post-9/11 Police Powers*, N.Y. TIMES, Aug. 27, 2002, at A12.

260. PATRIOT, *supra* note 18, § 203(b)(1), 115 Stat. at 280.

261. *Id.* § 203(b)(2), 115 Stat. at 280.

as foreign intelligence information whenever it relates to "the national defense or the security of the United States; or the conduct of the foreign affairs of the United States."[262] Section 203(d) mirrors the provisions in § 203(b) to apply the same authority and definitions to information obtained by intelligence services.[263]

These provisions were among the first used in the war against terrorism.[264] In fact, according to Attorney General Ashcroft, "information sharing and cooperation are critical to winning the war on terror and PATRIOT's capacity to increase these activities will be utilized to the fullest extent."[265] It appears that Ashcroft intends to eliminate completely any and all hindrances to full harmonization of law enforcement and counterintelligence operations, "both within [DOJ] and between [DOJ] and other federal intelligence agencies."[266] Although § 203 requires the Attorney General to adopt procedures in accordance with existing law and the Federal Rules, it provides no further guidance as to specific safeguards that the Attorney General should implement.[267] As this Note discusses in Part IV.B.1, DOJ has interpreted this ambiguity to allow complete dissolution of the old "wall" in any new procedures.

Finally, although the new law reiterates the National Security Act's prohibition against the CIA exercising police functions,[268] PATRIOT nevertheless gives the head of the CIA control in determining what information that agency may seek with FISA and how it should disseminate such information.[269] Essentially, this places the authority of the Director of the CIA above that of the Attorney General in determining the course of what often will be domestic

---

262. *Id.* § 203(b)(2)(c), 115 Stat. at 280.

263. *Id.* § 203(d), 115 Stat. at 281.

264. *See Hearing on DOJ Oversight, supra* note 1 (statement of John Ashcroft, Attorney General) ("Within hours of passage of the USA PATRIOT Act, we [DOJ] made use of its provisions to begin enhanced information sharing between the law-enforcement and intelligence communities.").

265. *Attorney General Ashcroft and Deputy Attorney General Thompson Announce Reorganization and Mobilization of the Nation's Justice and Law Enforcement Resources* (Nov. 8, 2001), *available at* http://www.justice.gov/ag/speeches/2001/agcrisisremarks11_08.htm (last visited Oct. 13, 2002).

266. *Id.* The Attorney General continued: "The Department of Justice is fully committed to breaking down the bureaucratic and cultural barriers that prevent meaningful coordination and cooperation between criminal law enforcement and the counterintelligence operations, both within the department and between the department and other federal intelligence agencies." *Id.*

267. PATRIOT, *supra* note 18, § 203, 115 Stat. at 280.

268. *See id.* § 403(d), 115 Stat. at 343-43 (requiring implementation of procedures that limit use of criminal history information supplied to Department of State and INS).

269. *See id.* § 901, 115 Stat. at 387 (amending National Security Act provision defining CIA Director's role to include "establish[ing] requirements and priorities for foreign intelligence information to be collected under [FISA]").

intelligence gathering operations, the fruits of which the government may use for intelligence and law enforcement purposes.[270] Given this provision, it is safe to say that the doctrine of separation is officially dead, and that a modern Big Brother is one step closer to reality.[271]

### *B. PATRIOT's Potential Threat to American Civil Liberties*

"[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."[272] Indeed, our nation's commitment to civil liberties has waned consistently in times of war: during the Civil War, the federal government suspended habeas corpus; during World War II it locked tens of thousands of Japanese-Americans in internment camps; in the throes of the Cold War, it blacklisted suspected communist sympathizers; and during the Vietnam War, it subjected dissidents to surveillance and harassment.[273] Today, our nation is very much at war, and as the preceding discussion should make clear, once again, we are departing dangerously from settled constitutional principles. PATRIOT represents such a significant break with the ideology that has guided our government in the conduct of national security surveillance that the unfortunate "pieces of our past [may] become prologue."[274]

During the Senate's consideration of PATRIOT, a number of Senators expressed concern that 9-11 had robbed both the public and Congress of commitment to traditional civil liberties.[275] This concern seems valid when considered in light of data from polls taken after 9-11, which showed that seventy-eight percent of respondents would accept increased security even at the expense of privacy protections.[276] Some legislators suggested that DOJ seized on public opinion to take advantage of the crisis and obtain a broad

---

270. *See* WHITEHEAD & ADEN, *supra* note 30, at 11 (noting that provision places "the CIA over the Justice Department and the FBI").

271. *See id.* (noting that this provision "turns on its head existing policy and practice that was put in place as a result of CIA abuses during the Cold War era and permits the CIA to begin once again to spy on American citizens").

272. 147 CONG. REC. S11,020 (2001) (statement of Sen. Feingold).

273. *See* 147 CONG. REC. S11,020 (2001) (statement of Sen. Feingold) (recounting examples of historical times during which United States government subrogated civil liberties).

274. 147 CONG. REC. S11,020 (2001) (statement of Sen. Feingold).

275. 147 CONG. REC. S11,020 (2001) (statement of Sen. Feingold).

276. *See* Kathryn Balint & Alex Roth, *Civil Liberties: Security Measures Pit Safety Against Privacy*, SAN DIEGO UNION-TRIB., Sept. 18, 2001, at A1 (noting results of NBC News/ Wall Street journal poll). The same percentage of those polled said they "would support surveillance of Internet communications; and 43 percent said they were willing to let the government listen in on phone calls without a court order." *Id.*

range of tools it had coveted for a long time.[277] Now that time mercifully has softened the shock and terror of 9-11, it is time to reevaluate our nation's willingness to trade privacy for security and consider PATRIOT with a more level head.

### *1. Implementation and Expansion of PATRIOT Beyond Terrorism: Fourth Amendment Concerns*

One of the most foreseeable dangers of the new Act is that increased access to the lower standards of FISA, combined with the statutory authority to share information, will tempt overzealous executive officials to invoke PATRIOT in areas beyond terrorism. DOJ already has opined that PATRIOT allows FISA's implementation in investigations that are *primarily* law enforcement operations as long as the investigation also serves a significant foreign intelligence end.[278] In May of 2002, DOJ moved the FISC to "vacate the minimization and 'wall' procedures in all cases now or ever before [that] [c]ourt."[279] Under DOJ's proposed new minimization procedures, "criminal prosecutors would . . . no longer be prohibited from 'directing or controlling' counterintelligence investigations involving use of the FISA *toward law enforcement objectives*."[280] Moreover, "criminal prosecutors would . . . be empowered to direct the use of FISA surveillances and searches *toward law enforcement objectives* by advising FBI intelligence officials on the initiation, operation, continuation and expansion of FISA authority from [the FISC]."[281]

In its first public opinion in its twenty-four-year existence, the FISC refused to accept DOJ's proposal. The court's reasoning is quite lucid:

> The 2002 [proposed] procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillances and Rule 41 searches. This may be because the government is unable to meet the substantive requirements of these law enforcement tools, or because their administrative burdens are too onerous. In either case, the FISA's definition of minimization procedures has not changed, and these procedures

---

277. *See* 147 CONG. REC. S11,021 (2001) (statement of Sen. Feingold) (characterizing original bill proposal from administration as containing provisions objectionable to notions of civil liberty). Senator Feingold called one such proposal "simply an effort on the part of [DOJ] to take advantage of the emergency situation and get something that they've wanted for a long time." 147 CONG. REC. S11,020 (2001) (statement of Sen. Feingold).

278. Susan Schmidt, *Recognition of Patriot Act Urged*, WASH. POST, Aug. 24, 2002, at A6.

279. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, No. 02-429, slip op. at 1 (U.S. F.I.S.C. May 17, 2002), *available at* http://www.dcd.uscourts.gov/FISA-02-429.pdf (last visited Aug. 26, 2002).

280. *Id.* at 25.

281. *Id.*

> cannot be used by the government to amend the Act in ways Congress has not.[282]

Withstanding the steamroller momentum of the Bush administration's efforts to expand its prerogative in how to fight the war on terror, the FISC interpreted PATRIOT as maintaining some vestige of the "wall."[283] Ultimately, the FISC refused to allow criminal prosecutors to appropriate the "legal advantages conceived by Congress to be used by U.S. intelligence agencies" and thereby substitute FISA for Title III.[284]

However, the FISC's unanimous decision did not deter Attorney General Ashcroft and DOJ, who subsequently applied for FISA authorization using the denounced minimization procedures.[285] When this application was denied, the Government then appealed to the Foreign Intelligence Surveillance Court of Review (FISCR).[286] In the first time the FISCR had convened since its creation in 1978,[287] the court overturned the FISC's decision, finding that PATRIOT had "largely erased whatever boundaries existed between counterintelligence and domestic law enforcement."[288] The FISCR decided "that the restrictions imposed by the [FISC] are not required by FISA or the Constitution."[289] Despite its thorough fifty-six page decision, which addressed much of the case history considered in this Note, the FISCR's ultimate constitutional conclusion does not inspire confidence:

> We acknowledge . . . that the constitutional question presented by this case – whether Congress's disapproval of the primary purpose test is consistent with the Fourth Amendment has no definitive jurisprudential answer . . . . Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA if they do not meet the minimum Fourth Amendment warrant requirements standards, certainly come close. We, therefore, believe firmly, . . . that FISA as amended is constitutional because the surveillance it authorizes are reasonable.[290]

---

282. *Id.* at 22.

283. *See id.* at 23-25 (discussing dangers of Attorney General's proposed procedures).

284. *Id.* at 24.

285. *See In re* Sealed Case, No. 02-001, 2002 WL 31546991 at *5 (U.S. F.I.S.C.R. Nov. 18, 2002) (hereinafter FISCR Decision) (explaining how May 17th opinion was not order actually appealed, but was "basic decision before" FISCR).

286. *Id.*

287. *Id.* at *1.

288. Jess Bravin, *Ruling Eases Terror-Suspect Pursuit*, WALL ST. J., Nov. 19, 2002, at A2.

289. FISCR Decision at *1.

290. *Id.* at *55.

With this undeniably tentative constitutional pronouncement, the FISCR has cleared the way for nearly unfettered implementation of FISA surveillance in a variety of contexts beyond terrorism per se.[291]

The area most likely to see utilization of the tools provided to fight the war on terror is narcotics enforcement.[292] From the beginning, "officials have tried to link the new war on terror to the old war on drugs."[293] It seems clear that the Bush administration intends to merge antiterrorism efforts with drug interdiction. In his February 2, 2002 remarks on the 2002 National Drug Policy, President Bush drew an unambiguous connection:

> You know, I'm asked all the time, how can I help fight against terror? What can I do, what can I as a citizen do to defend America? Well, one thing you can do is not purchase illegal drugs. Make no mistake about it, if you're buying illegal drugs in America, it is likely that the money is going to end up in the hands of terrorist organizations. Just think about the Taliban in Afghanistan – 70 percent of the world's opium trade came from Afghanistan, resulting in significant income to the Taliban, significant amount[s] of money to the people that were harboring and feeding and hiding those who attacked and killed thousands of innocent Americans on September the 11th. *When we fight drugs, we fight the war on terror.*[294]

The Bush administration even pitched its drugs-to-terror connection during the television coverage of the 2002 Super Bowl, when the Office of National

---

291. *See id.* at *36 ("That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself."). The FISCR's decision came down only days before the final publication deadline for this Note. Thus, the instant consideration of the decision and its ramifications is, unavoidably, constrained. However, the import and divisiveness of this decision is clear from the reactions within the government. For instance, Attorney General Ashcroft "called the ruling 'a victory for liberty, safety and the security of the American people,'" while the senior Democrat on the House Judiciary Committee, John Conyers, labeled the ruling "despicable" and suggested that it was another example of how the Bush administration "is dismantling the basic rights afforded to every American under the Constitution." Bravin, *supra* note 288. An interested reader should consider the FISCR's opinion in full for a more complete perspective.

292. *See* Remarks of President Bush on 2002 National Drug Control Policy, East Room, Feb. 12, 2002, *at* http://www.whitehouse.gov/news/releases/2002/02/20020212-8.html [hereinafter *National Drug Control Policy Remarks*] ("[T]he drug trade supports terrorist networks. When people purchase drugs, they put money in the hands of those who want to hurt America, hurt our allies. Drugs attack everything that is the best about this country, and I intend to do something about them.").

293. Tim Golden, *The World: A War on Terror Meets a War on Drugs*, N.Y. TIMES LATE EDITION, Nov. 25, 2001, at § 4, p.4, col.1.

294. *National Drug Control Policy Remarks*, *supra* note 292 (emphasis added).

Drug Control Policy spent nearly $3.5 million to produce and air two commercials during the game.[295] One of the spots put the issue thus: "Where do terrorists get their money? . . . If you buy drugs, some of it might come from you."[296] And where does the war on drugs get its money? The *Wall Street Journal* reported recently that "[t]he Drug Enforcement Administration will receive $35 million from the Justice Department for counterterrorism and intelligence support."[297]

Regardless of whether there is justification for the correlation between drug use and terrorism, it seems clear that the executive intends to treat the two problems as like evils. Drug-enforcement operations account for nearly eighty percent of criminal surveillance applications,[298] and as the administration begins to cast efforts to combat narcotics as efforts to fight the war on terror, it is entirely possible – even likely – that it will invoke PATRIOT's new surveillance authority in drug-enforcement operations. In such a context, the rubberstamp approval history of the FISC court, combined with the inaccessibility of FISA applications to those who are targets, could effect a circumvention of the Fourth Amendment for heretofore common criminal investigations.

### *2. Inadequate Safeguards*

Although PATRIOT dramatically increases the ability of the government to make use of questionable surveillance procedures, it provides little in the way of new safeguards. As discussed in Part III.A.2, herein, many consider the FISC too entrenched within the culture of those seeking to protect our nation to provide an adequate constitutional check against overzealous or

---

295. *Anti-Drug Ads Play the Terror Card; Linking Street Buys to Funding Militant Networks Draws Fire*, SAN. FRAN. CHRON., Feb. 4, 2002, at A1.

296. *Id.* The San Francisco Chronicle article notes that the ads were met with criticism. The paper quoted Matthew Briggs, an assistant director of New York's Drug Policy Alliance, as saying, "It's a cynical, cheap shot to take in the current political environment, to make it sound like a kid who smokes pot is responsible for putting cash in the hands of Osama bin Laden is ludicrous." *Id.* The administration's conclusion that drug trafficking *finances* terrorism, fits nicely with FISCR's explicit endorsement of FISA surveillance for such circumstances. *See supra* note 291 (recounting FISCR's "bank robbery" example).

297. *DEA Will Get $35 Million for Afghanistan Programs*, WALL ST. J., Feb. 5, 2002.

298. *See* Administrative Office of the U.S. Courts, Wiretap Report 2000: Table 7 Authorized Intercepts Granted Pursuant to 18 U.S.C. 2519 as Reported in Wiretap Reports for Calendar Years 1990-2000 (recording that of 12,039 authorized wiretaps, 8,495 cited narcotics as primary offense), *available at* http://www.uscourts.gov/wiretap00/contents.html (last visited March 4, 2001); *see also* Young, *supra* note 25, at 1026 ("Wiretaps were sought predominantly for narcotics-related offenses." (citation omitted)).

improper executive action.[299] Moreover, even if the FISC meets its oversight burden, it still must rely on the executive's representations, which are not necessarily reliable. In fact, in September of 2000 the government admitted to committing some seventy-five "misstatements or omissions of material facts" in FISA surveillance applications.[300] Because of the privileged nature of the information often contained in FISA applications and orders, there is little chance that anyone in the future will know of executive abuse of PATRIOT, and any exposure certainly will not occur before the damage is done.

The threat to civil liberties is exacerbated by a policy that has become increasingly clear: The Bush administration, and especially Attorney General Ashcroft, want to limit the public's and Congress's access to anything pertaining to terrorism investigations. First, an exclusionary provision is built into PATRIOT that allows the delay of reports to Congress on intelligence matters.[301] Second, Ashcroft has voiced resistance to congressional meddling in hearings reviewing the administration's anti-terrorism policy and asserted the President's constitutional authority to act on his own.[302] This resistance has gathered steam and secrecy has become a clear objective of the administration.[303] This emphasis on secrecy further limits oversight efforts and makes discovery of Fourth Amendment abuses much less likely, thereby increasing the particular danger that Justice Powell identified in *Katz*: that "unreviewed

---

299. *See supra* notes 185-86 and accompanying text (discussing assertions that FISC is puppet of executive).

300. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, No. 02-429, slip op. at 16 (U.S. F.I.S.C. May 17, 2002), *available at* http://www.dcd.uscourts.gov/FISA-02-429.pdf (last visited Aug. 26, 2002); Schmidt, *supra* note 278, at A6; Shenon, *supra* note 259, at A12.

301. *See* PATRIOT, *supra* note 18, § 904, 115 Stat. at 387-88 (granting authority to delay temporarily reports to Congress on intelligence matters).

302. *See Hearing on DOJ Oversight*, *supra* note 1 (statement of John Ashcroft, Attorney General) ("[C]ongress's power of oversight is not without limits. . . . In some areas, however, I cannot and will not consult you. . . . For centuries, Congress has recognized [the power of the President as Commander-in-Chief] and the Supreme Court has never held that any Congress may limit it.").

303. *See* Don Wycliff, *Top Secret: Just Whose Government Is It, Anyway?*, CHI. TRIB., Jan. 17, 2002, at 23 (noting Bush administration's "fondness for secrecy" and Ashcroft's "Oct. 12 memorandum to executive agencies" urging restriction of grants of information under Freedom of Information Act). This article notes that the implication of Ashcroft's memo is "that freedom of information is opposed to or in competition with other important values such as 'national security,' 'functional and efficient' government, 'enhancing the effectiveness of our law enforcement agencies,' protecting 'sensitive business information' and 'preserving personal privacy.'" *Id.*; *see also* Eric J. Sinrod, *Defanging the Freedom of Information Act*, N.Y.L.J., Jan. 22, 2002, at 5 (noting that Ashcroft's new policy must "not frustrate the core purpose of the FOIA shining a light on 'what the government is up to'").

executive discretion may yield too readily to pressures to obtain incriminating evidence."[304]

It is important to note that secrecy also limits the effectiveness of the internal checks contained within PATRIOT. Section 223 of PATRIOT provides for civil liability in the event of unauthorized disclosure,[305] but in the context of national security surveillance there is little or no recourse for citizens injured by executive impropriety.[306] Often, it is impossible to sustain a claim "for damages based on statutory and constitutional violations" inflicted by the participants in national security surveillance.[307] Finally, the limitations to new surveillance authority imposed by sunset provisions[308] do nothing to compensate those whose liberties the government treads upon before PATRIOT's sun goes down.

### *V. Conclusion*

All of the United States government's efforts to combat terrorism across the globe have done little to allay the lingering fear that 9-11 branded on the heart of our nation. The fact is that each nightly newscast brings more concerns. Perhaps the most difficult aspect of the war on terror is that we are fighting a faceless enemy. Terrorism comes in many forms, carried out by men and women of all nationalities and creeds. However, all terrorists share one thing in common – brutality. The United States is fighting a war against an enemy that will force a captured journalist to sit in front of a camera and recite that he is a Jew and that his father was a Jew, as the enemy's agent slips up from behind and slits the journalist's throat.[309] The war on terror is a war against a hatred that is hard to comprehend, a hatred strong enough to lead people to offer willingly their lives in order to kill others.

---

304. *Keith*, 407 U.S. at 314.

305. PATRIOT, *supra* note 18, § 223, 115 Stat. at 293-94.

306. *See* Halkin v. Helms, 690 F.2d 977, 984 (D.C. Cir. 1982) [Halkin II] ("As a result of that ruling [Halkin I], plaintiffs' claims against the NSA and several individual officials connected with that agency's monitoring activities could not be proved, and the complaint as to those defendants was dismissed."); Halkin v. Helms, 598 F.2d 1, 10 (D.C. Cir. 1978) [Halkin I] (upholding Secretary of Defense's claim of state secret privilege and ruling that NSA did not have to disclose interception of plaintiffs' communications).

307. *Halkin II*, 690 F.2d at 990 (emphasis omitted).

308. *See* PATRIOT, *supra* note 18, § 224, 115 Stat. at 294 (ceasing effect of parts of Title as of December 31, 2005).

309. John Ward Anderson & Peter Baker, *Killers Likely Never Intended to Free Pearl; Abduction and Videotaped Slaying of Reporter Meant to Send Message, Pakistani Police Say*, WASH. POST, Feb. 23, 2002, at A16.

It is hardly surprising, then, that we find ourselves reevaluating what it means to be free and how far we are able to go to protect our civil liberties without endangering our lives. The world is a very different place now than it was before September 11, 2001, and we must recognize that this new world may require an entirely different approach. PATRIOT's provisions largely remove modern national security surveillance efforts from the principles set forth in *Katz*, *Keith*, and their progeny. However, that does not mean that PATRIOT's provisions are necessarily evil; evil has made them a necessity. Further, the jurisprudence of the foreign intelligence exception and of FISA, as well as the magnitude of the dangers facing our country, make it likely that PATRIOT will survive challenges in the courts.

However, one cannot deny the expansive new authority PATRIOT vests in the executive and the potential for abuse that this authority necessarily brings; PATRIOT cracks the door for Big Brother. As with any new authority, there is a new level of responsibility, not just for the executive, but also for Congress and the public in overseeing the implementation of PATRIOT. We must never forget Justice Brandeis's warning that "[t]he greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."[310]

PATRIOT is an understandable and perhaps justifiable response to the grave threat painfully realized on 9-11. However, we should be careful not to allow our anti-terrorist fervor to spill over into the general fight against crime. To do so is to ignore the centuries of legislation and jurisprudence that have made our criminal justice system the envy of the civilized world. Recognizing the inevitability of a new approach to fighting terrorism should not force us to lose the resolve to protect our civil liberties. We must bear in mind that "the history of the last five decades shows that attacks on privacy are not an anomaly. When government has the power to invade privacy, abuses occur."[311] The challenge facing our country is daunting, but we should seek to meet it head on. It is time for us to rethink our prerogatives and consider how best to bring our democratic society into the new millennium without sacrificing two and a half centuries of freedom.

---

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

311. Young, *supra* note 25, at 1077 (quoting WHITFIELD DIFFIE & SUSAN LANDAN, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 148 (1998)).