Case Western Reserve Journal of International Law

Volume 35 | Issue 1

2003

Thwarting Ideological Terrorism: Are We Brave Enough to Maintain Civil Liberties in the Face of Terrorist Induced Trauma

Kelly R. Cusick

THWARTING IDEOLOGICAL TERRORISM: ARE WE BRAVE ENOUGH TO MAINTAIN CIVIL LIBERTIES IN THE FACE OF TERRORIST INDUCED TRAUMA?

Kelly R. Cusick[†]

I. INTRODUCTION

On September 11, 2001, terrorists hijacked four commercial passenger jets, two crashing into the World Trade Center, one into the Pentagon[1] and one into an open field in Pennsylvania. This act of terrorism killed thousands of innocent people and attempted to weaken the American spirit by attacking one institution that symbolizes American economic strength and another that protects American freedoms.[2] The United States realized a new and heightened vulnerability to terrorism. In response, the Bush Administration has focused an overwhelming amount of attention on combating terrorism.[3] On October 26, 2001 the government passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT ACT"),[4] which greatly expands the power of the federal government to investigate, detain, and deport those people who the government suspects are linked to terrorist activity and other crimes.[5]

[†] J.D., Case Western Reserve University School of Law (2003); B.A., Colgate University (2000). I would like to thank Hiram E. Chodosh, Director of the Fredrick K. Cox International Law Center, and the Executive Board of the Case Western Reserve University Journal of International Law for their support, understanding, and guidance.

[1] Mark Hall & Lucas Mearian, *IT Focus Turns To Disaster Recovery*, *at* http://www.cnn.com/2001/TECH/industry/09/11/disaster.recovery.idg/index.html (last visited Oct. 7, 2002).

[2] *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Committee on the Judiciary*, 107th Cong. (Sept. 24, 2001) (statement of F. James Sensenbrenner).

[3] NATIONAL SECURITY ARCHIVE ELECTRONIC BRIEFING BOOK NO. 55 VOLUME I: TERRORISM AND U.S. POLICY (Jeffery Richelson & Michael L. Evans eds., Sept. 21, 2001), *at* http://www.gwu.edu/~nsarchiv/NSAEBB55/index1.

html.

[4] Bill Summary & Status for the 107th Congress H.R. 3162, *at* http://www.thomas.loc.gov/cgi-bin/bdquery/z?d107:HR0312:@@@L&summ2=m& (last visited Oct. 7, 2002).

[5] John Lancaster & Jonathan Krim, *Aschcroft Presents Anti-Terrorism Plan to Congress*, WASH. POST, Sept. 20, 2001, at A24.

In enacting this bill, Congress considered how the United States could better protect itself from future terrorist attacks, as well as how those protections would affect civil liberties.[6] Congress tried to strike a balance between the need to protect the country from terrorists and the need to protect Americans' civil and constitutional liberties.[7]

Regrettably, Congress did not strike an acceptable balance. The Act created to protect against terrorism extends beyond that limited goal, hindering the Act's effectiveness and impinging on the civil liberties of Americans more than necessary. As Professor Chimerinsky stated, "Some loss of freedom may be necessary to ensure security; but not every sacrifice of liberty is warranted . . . The central question must be what rights need to be sacrificed, under what circumstances, and for what gain."[8] The United States of America needed legislation to increase protection against future terrorist attacks, but enhancing surveillance powers, as done in Title II of the USA PATRIOT ACT, creates many opportunities for civil liberty violations, and is also largely ineffective. Rather than immediately granting broader surveillance powers, the government should have first improved the management and organization of many government agencies.

This paper focuses solely on Title II of the legislation, Enhanced Surveillance Procedures. Section II provides an overview of the pre-September 11th intelligence surveillance procedures of the United States. Section III evaluates five provisions of Title II regarding their effectiveness and constitutionality and suggests amendments that remedy the problems the provisions pose. Section IV discusses less intrusive steps the government should have considered before extending surveillance powers that violate American civil liberties.

II. SURVEILLANCE PROCEDURES

A. Pre-USA PATRIOT ACT Intelligence Surveillance

United States policy on combating terrorism has evolved during the past thirty years.[9] In 1981, former President Reagan's Secretary of State,

---

[6] *See* CONG. REC. S10569 (daily ed. Oct. 11, 2001) [hereinafter *Debate: Uniting and Strengthening America Act*] (statement of Sen. Russell D. Feingold, Member Senate Comm. on the Judiciary).

[7] *Id.* at S10548 (statement of Sen. Leahy).

[8] *Protecting Constitutional Freedoms in the Face of Terrorism: Hearing Before the Subcomm. On the Constitution, Federalism, and Property Rights of the Senate Comm. on the Judiciary,* 107th Cong. 2 (2001) [hereinafter *Hearings*] (statement of Russell D. Feingold, Chairman, Subcomm. On the Constitution, Federalism, and Property Rights)..

[9] U.S. General Accounting Office, *Report to Congressional Committees: Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822, 5 (Sept. 2001), *available at:* http://www.gao.gov/.

Alexander Haig, announced opposition to terrorism as a focus of the administration, and each successive administration has paid significant attention to terrorism.[10] Prior to September 11th, federal law already gave leeway to the government in combating terrorism to a degree that few Americans realized.[11] In order to understand the overbreadth and ineffectiveness of the powers granted in Title II of the USA PATRIOT ACT, the focus of this Note's analysis, one needs to understand the previous law pertaining to intelligence surveillance procedures.

Until the mid-1970s, the executive branch had regularly conducted electronic surveillance under the guise of national security without a court order.[12] The Fourth Amendment, designed to protect individual privacy interests from certain kinds of governmental intrusion, was not extended to include wiretaps until 1967.[13] And even then, the court expressly exempted national security surveillance from the reach of its decision requiring a warrant for electronic surveillance.[14] Five years later, the Supreme Court held that to be in compliance with the Fourth Amendment, electronic surveillance for purposes of domestic security required a warrant.[15] But again, the court explicitly declined to address whether electronic surveillance of foreign governments or their agents also required a prior warrant.[16] This distinction between domestic security and national security caused potential confusion for both law enforcement officers and courts by exacerbating the ambiguity of surveillance for national security purposes and indicated that surveillance law needed to be more explicit.

In addition to unclear case law, the discovery of many governmental abuses of authority in the mid-1970s, including Watergate, created an antagonistic mood toward the use of executive power, especially regarding

---

[10] *See* Richelson & Evans, *supra* note 3. Although opposition to terrorism never really did become the primary focus of the Reagan administration or following administrations, each paid significant attention to the issue and produced many important documents that shed light on the policy choices faced today.

[11] Brigid McMenamin, *Land of the Free: Repeal of Bill of Rights? Authorities already have a lot of legal tools to fight terrorism*, FORBES, Oct. 15, 2001, at 56.

[12] *Hearings, supra* note 8, at 17 (statement of Dr. Morton H. Halperin, Senior Fellow, The Council of Foreign Relations, and Chair, Advisory Board, Center for National Security Studies).

[13] Katz v. United States, 389 U.S. 347, 350 (1967) (holding, when the privacy a person justifiably relies upon was invaded when wiretapped, wiretapping constitutes a search and seizure within the meaning of the Fourth Amendment). *Id.* at 353. Because of this holding, law enforcement officials had to comply with the more strict Fourth Amendment requirements when performing electronic surveillance.

[14] *Id. at* 358 n. 23.

[15] United States v. United States District Court for Eastern District of Michigan, 407 U.S. 297, 309 (1972).

[16] *Id.* at 321-22.

intelligence and national security related activities.[17] The congressional hearings commonly known as the Church Committee hearings, revealed instances where United States intelligence agencies had used unfettered warrantless electronic surveillance on United States citizens who were unrelated to any source of foreign intelligence information and unassociated with any criminal activity, all in clear violation of individual privacy rights.[18] The committee concluded that such abuse of executive discretion resulted from lack of clear congressional or judicial standards.[19]

To limit this unregulated discretion, in 1978 the government created the Foreign Intelligence Surveillance Act ("FISA") to conduct electronic surveillance for national security purposes.[20] FISA granted the Federal Bureau of Investigation ("FBI") and the Central Intelligence Agency ("CIA") extremely broad authority both to investigate terrorism and to conduct counter intelligence against foreign nationals within the United States and against American citizens suspected of involvement with foreign terrorist groups.[21]

Congress deliberated about the extent of authority to which national security surveillance was entitled under FISA and reached a balance that was widely considered to allow for adequate protection while preserving civil liberties.[22] After years of debate, Congress and the executive branch made substantial compromises to reach an agreement on an effective regulation.[23] The executive branch was entitled to conduct electronic surveillance for national security purposes under a standard less strict than the probable cause standard of a criminal investigation.[24] Surveillance could also be kept a secret, without providing the notice required in

---

[17] Americo Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978,* 137 U. PA. L. REV. 793, 806 (1989).

[18] *Id.* at 806-07.

[19] *Id.* at 807.

[20] *Hearings, supra* note 8, at 17.

[21] *Hearings*, *supra* note 8, at 30 (statement of Jerry Berman).

[22] *See, e.g.,* U.S. v. Pelton, 835 F.2d 1067 (Md. 1987), cert. denied, 486 U.S. 1010 (1988) (stating that, "Foreign Intelligence Surveillance Act (50 USCS 1901 et. Seq.) does not violate Fourth Amendment, since statutory safeguards provide sufficient protection for rights of individual guaranteed by Fourth Amendment within context of foreign intelligence activities, where governmental interests in gathering foreign intelligence are of paramount importance to national security and may differ substantially from those presented in normal criminal investigations; and prior to issuance of surveillance order, judicial review is required and there are limitations to exercise of that authority and conduct of surveillance."). 50 U.S.C.S. § 1802 interpretative notes and decisions, ann. 2.

[23] Cinquegrana, *supra* note 17, at 794.

[24] United States v. Truoung Dihn Hung, 629 F.2d 908, 914 n. 4 (4th Cir. 1980).

criminal investigations.[25] In return for this broader authority, judicial supervision was required.[26] Also, FISA required agents to minimize the interception of irrelevant information.[27] Most importantly, FISA procedures could not be used by the government when conducting criminal investigations.[28]

Protecting national security from foreign threats requires more expansive government intelligence powers than those allowed in criminal investigations. Rather than limiting the discretion of law enforcement, as is done in criminal investigations, the FISA grants broad discretion for the intelligence community.[29] These broader powers were required because countering a foreign intelligence threat requires more speed and furtiveness than a domestic criminal investigation.[30] In addition, the executive branch possesses the needed expertise to determine how to conduct foreign intelligence surveillance, while the judicial branch, ordinarily in charge of granting surveillance warrants, lacks similar experience in making complex decisions involved in foreign intelligence investigations.[31]

The constitutionality of the framework established by FISA and its implementation has been repeatedly scrutinized by federal courts, usually in the context of terrorism and espionage.[32] A representative case[33] concluded that FISA created a "constitutionally adequate balancing of individual's Fourth Amendment rights against the nation's need to obtain intelligence

---

[25] 50 U.S.C. § 1806 (a) (1994).

[26] Cinquegrana, *supra* note 17, at 812. Surveillance activities needed to be authorized in advance by one of seven federal district court judges designated by the Chief Justice of the Supreme Court as members of the Foreign Intelligence Surveillance Court ("FISC").

[27] *Hearings*, *supra* note 8, at 17 (statement of Dr. Halperin). The targeted foreign power or agent must use the location at which surveillance is directed, and the method of surveillance must adequately minimize the acquisition, retention, and dissemination of information concerning unconsenting United States persons, while preserving the government's ability to obtain the intelligence it seeks in order for an FISC judge to approve the surveillance. Cinquegrana, *supra* note 17, at 812-813.

[28] *Hearings, id.* at 18 (statement of Dr. Halperin). When conducting criminal investigations, Title III of the Omnibus Crime Control and Safe streets act of 1968 applied.

[29] *Id.* at 30. The intelligence community was permitted to place wiretaps, install bugs, and conduct secret searches without showing probable cause of criminal conduct, without giving notice, or even without turning the results of the surveillance over for later review. *Id.* Within thirty minutes, investigators could get warrants to tap phones, search homes or forgo the warrants all together in times of emergency. McMenamin, *supra* note 11, at 56.

[30] *See* Zweibon v. Mitchell, 516 F.2d 594, 704 (D.C. Cir. 1975) (Wilkey, J., concurring and dissenting).

[31] *See* New York Times Co. v. United States, 403 U.S. 713, 727-30 (1971) (Stewart, J. concurring).

[32] Cinquegrana, *supra* note 17, at 816.

[33] *Id.* at 817.

information."[34] The court viewed the framework of FISA as an appropriate exercise of Congressional political judgment and as rationally related to the purpose of protecting the United States from actions of foreign powers.[35] The FISA process and its implementation have withstood substantial judicial scrutiny.[36]

FISA embodies legal principles that developed over decades through contemplative Supreme Court decisions and deliberate actions performed by Congress and the Executive branch.[37] This development illustrates that by taking the time both to fully understand how the act will function in society and to compromise when creating the balance of national security with civil liberties, we can find solutions that respect civil liberties but also facilitate the attainment of necessary intelligence information. The drafters of the USA PATRIOT ACT did not take such time in its creation. Accordingly, many of its provisions did not achieve the balance of providing national security while protecting civil liberties.

B. The Importance of Civil Liberties in Relation to Surveillance

Guaranteeing the security of the United States is the most fundamental governmental objectives and intelligence surveillance plays a critical role in the protection of national security.[38] However, protecting civil liberties is of great importance. That is why FISA went through years of debate. The values of the Constitution of the United States have united the country for more than 200 years.[39] The framers designed the Constitution to protect civil liberties in times of war as well as in times of peace.[40] They had recently won the Revolutionary War; times were not comfortable or easy, and enemies posed a real threat.[41] However, protecting civil liberties remained a central goal. Similarly, the current threat of terrorism cannot now be used as justification to disregard civil liberties provided by the Constitution.

---

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

[35] *Id.* at 75-76.

[36] Cinquegrana, *supra* note 17, at 820.

[37] *Id.* at 794.

[38] See Louis A Chiarella & Michael A. Newton, *So Judge, How Do I Get That FISA Warrant?: The Policy and Procedure for Conducting Electronic Surveillance*, 1997 ARMY LAW 25, 25-26 (1997).

[39] *Hearings: The United States Judiciary Committee Subcommittee on the Constitution, Federalism, and Property Rights* (Oct. 3, 2001) (statement of Senator Patrick Leahy).

[40] *Hearings, supra* note 8, at 1-3 (statement of Hon. Russell D. Feingold).

[41] *Id.*

American ideals and values must be respected to maintain the strength of the United States.[42] Commitment to the principles of the Constitution in the face of terrorist atrocities will serve justice and demonstrate the strength of the United States to the world.[43] Even before September 11th, the government acknowledged that terrorists hope to provoke responses that undermine the Constitution of the United States.[44] A report published before the USA PATRIOT ACT argued that counterterrorism policies must be effective, but must also respect the democratic traditions.[45]

The USA PATRIOT ACT could have profound implications on the democracy of the United States.[46] Privacy involves the relationship of the individual to the state, the most fundamental aspect of a government.[47] Since the beginning of the United States, "Americans have been committed to the idea that people have the right to control how much information about their thoughts, feelings, choices and political beliefs is disclosed."[48] Privacy acts as the boundary that provides protection from the outside world and maintains human dignity.[49] Privacy works to shield minorities and outsiders from persecution,[50] something America prides itself in providing. "By reducing our commitment to privacy, we risk changing what it means to be Americans."[51]

History illustrates that, in times of peril, hastily taken measures often weaken governmental restrictions against coercive and intrusive powers and often infringe on civil liberties without substantially enhancing security.[52] Throughout United States history, the country allowed civil liberties to be sacrificed in face of what seemed to be legitimate exigencies of war: the Alien and Sedition Acts, the internment of Japanese-Americans during World War II, the blacklisting of supposed communist sympathizers during the McCarthy era,[53] and the government's surveillance of civil rights

---

[42] *See id.* at 16 (statement of Senator Patrick Leahy).

[43] *See id.*

[44] *See Countering the Changing Threat of International Terrorism: Report of the National Commission on the Terrorism,* 106th Cong. (June 15, 2000)..

[45] *See id.*

[46] Mike France, Heather Green, Jim Kerstetter, Jane Black, Alex Salkever & Dan Carney, *Privacy in an Age of Terror: To Track Terrorists, Government Snoops will have to Track You, Too*, BUSINESS WEEK, Nov. 5, 2001, at 83.

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.* at 84.

[52] *Hearings*, *supra* note 8, at 26-28 (statement of Jerry Berman).

[53] *Id.* at 1-3 (statement of Russell D. Feingold).

leaders in the 1960s.[54] These abuses should not be forgotten in this war against terrorism, but rather used as a lesson that the risk of governmental abuse is substantial.[55] As Louis D. Brandeis explained, "[e]xperience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[56] This history of abuse indicates that civil liberty violations will likely be a reality if governmental powers are not carefully constructed with safeguards. Title II of the USA PATRIOT ACT lacks effective safeguards.

III. TITLE II: ENHANCED SURVEILLANCE PROCEDURES

The stated purpose of the USA PATRIOT ACT is to protect America from terrorism.[57] Accordingly, each provision of the Act should be narrowly tailored to improve the government's ability to detect and prevent terrorist actions. However, many of Title II's provisions grant overly broad surveillance powers that extend beyond preventing terrorism. This section analyzes five provisions of Title II: foreign intelligence information, pen registration and trap and trace devices, roving surveillance authority under FISA, authority for delaying notice, and the sharing of information. The analysis examines whether the provisions are unconstitutional, ineffective or both, and poses remedies for their shortcomings.

A. Foreign Intelligence Information

Prior to September 11th, the intelligence surveillance legislation, the FISA, distinguished criminal investigation surveillance from intelligence surveillance. If "the purpose" of a search or wiretap was "to obtain foreign intelligence information," not to pursue a criminal investigation, the lesser restraints of FISA applied,[58] rather than the stricter requirements of Title III

---

[54] Manuel Perez-Rivas, *Anti-Terrorism Proposals Worry Civil Libertarians* (Sept. 25, 2001), *at* http://www.cnn.com/2001/US/09/25/inv.civil.liberties/.

[55] *Id.*

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

[57] Attorney General John Ashcroft, the Act's primary drafter, stated, "[O]ur single objective is to prevent terrorist attacks by taking suspected terrorists off the street." Attorney General John Ashcroft, Prepared Remarks from the US Mayors Conference (Oct. 25, 2001). In order to achieve this, Ashcroft explained that the legislation needed to provide law enforcement with the necessary tools to identify, dismantle, disrupt and punish terrorist organizations before they strike again. *Id.*

[58] 50 U.S.C.S. § 1804(a)(7)(B); 50 U.S.C.S.1823 (a)(7)(B) (1996).

of the Omnibus Crime Control and Safe Streets Act ("Omnibus Act").[59] Under the Omnibus Act, a neutral magistrate must find probable cause that a serious crime has been, or is about to be committed in order to issue a warrant for electronic surveillance.[60] Requiring probable cause helps to ensure that wiretaps and search warrants only invade the privacy of those likely to be involved in the crime.[61] In addition, notice must be provided to the target of surveillance during electronic and physical searches in criminal cases, even if the information gathered does not result in prosecution.[62] Thus, prior to September 11th, when gathering surveillance information for criminal prosecution purposes, law enforcement discretion was restricted by various safeguards.

FISA intelligence surveillance procedures lack similar safeguards protecting civil liberties. FISA searches do not hinge upon showing probable cause.[63] The FISA gives the FBI authority to conduct secret wiretaps and physical searches; notice is not required.[64] Without providing notice, law enforcement agents can break into a party's home or business and conduct a search.[65] The party will never know of the search, unless criminal prosecution follows.[66] Because the search warrants are secret, the target of a FISA surveillance cannot obtain discovery of the warrant, and is thereby prevented from challenging the search if done improperly.[67] As previously discussed, in order for the FISA to protect the national security of the country from foreign threats, it must grant broad discretion to law enforcement officials. However, because FISA procedures are invasive, they were limited to the narrow area of intelligence surveillance, not criminal investigations.

1. SECTION 218 OF THE USA PATRIOT ACT

Section 218 blurs this essential distinction between criminal and intelligence surveillance. It requires only that "a significant purpose" of a

---

[59] Cinquegrana, *supra* note 17, at 800 (defining more clearly the proper use of electronic surveillance in criminal investigation).

[60] *Id.* at 801.

[61] THE AMERICAN CIVIL LIBERTIES UNION, *How The Anti-Terrorism Bill Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases* [hereinafter ACLU], *at* http://www.aclu.org/congress/1102301i.html (last visited Oct. 7, 2002).

[62] Chiarella, *supra* note 38, at 27.

[63] 50 U.S.C.S. § 1804 (1996).

[64] 50 U.S.C. § 1805 (a) (1994); 50 U.S.C. § 1825(a) (1994).

[65] ACLU, *supra* note 61.

[66] 50 U.S.C. § 1825(c) (1994).

[67] ACLU, *supra* note 61.

search or wiretap be "to obtain foreign intelligence information."[68] The addition of the word "significant" eliminates the previous FISA civil liberty safeguard that separated criminal surveillance from intelligence surveillance. It allows a search to be performed under the FISA guidelines even if the motivation is to get criminal evidence, not foreign intelligence information. This change now allows the FBI to conduct secret searches or to secretly record telephone conversations without probable cause when their primary purpose is to obtain criminal information, not to gather foreign intelligence.[69] Section 218 jeopardizes the civil liberties of Americans who pose no terrorist threat.

2. SECTION 218 IS UNCONSTITUTIONAL

Although the FISA requires fewer civil liberty protections, it is constitutional. The Fourth Amendment of the United States Constitution requires the government to prove to a judicial officer that it has probable cause of a crime before it conducts an invasive search to find evidence of that crime.[70] When creating the FISA, Congress provided safeguards to ensure that the broad authority to search for intelligence would not be used to evade the criminal probable cause requirement.[71] Congress required that the search or wiretap's purpose be to gather foreign intelligence.[72] If the primary purpose was a criminal investigation, the law enforcement officials had to first prove the higher standard of probable cause.[73] Investigating criminal activity cannot be the primary purpose of FISA surveillance.[74] As emphasized in a case prior to the USA PATRIOT ACT, the FISA "is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches."[75] It is not to be used as a tool to enable law enforcement officials to perform surveillance for the purpose of a criminal investigation when they lack probable cause.

However, the change made by Section 218 authorizes unconstitutional activity by impinging on the Fourth Amendment protection that requires probable cause. Section 218 now provides law enforcement officials with a vehicle to avoid probable cause when conducting criminal investigation surveillance. As long as law enforcement officials can find some aspect of

---

[68] H.R. 3162 § 218, 107th Cong (2001) (enacted).

[69] ACLU, *supra* note 61.

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

[71] ACLU, *supra* note 61.

[72] 50 U.S.C. § 1804(a)(7)(B) (1994), *amended by* Pub. L. No. 107-56 and 50 U.S.C. § 1823 (a)(7)(B) (1994).

[73] ACLU, *supra* note 61.

[74] United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991).

[75] *Id.* at 572.

the surveillance relating to intelligence gathering, the surveillance is now very likely to be allowed under FISA standards even if the surveillance is primarily conducted for criminal investigation purposes. The word "significant" is not enough of a safeguard to protect the probable cause requirement for criminal investigations.

3. SECTION 218 IS INEFFECTIVE

Section 218 not only creates the opportunity for law enforcement agents to avoid constitutional requirements designed to protect civil liberties, but also fails to effectively prevent terrorism. Instead of extending intelligence authority to catch more terrorists, Section 218 may enable terrorists to escape conviction. Case law indicates that courts will probably exclude the evidence gathered under this new authority because probable cause was not met in criminal investigations.[76] The Department of Justice could not cite one instance in which a court has admitted evidence gathered from a FISA search conducted primarily for criminal purposes.[77] One court explained that the original FISA requirement that gathering foreign intelligence information had to be the purpose of the surveillance was the proper test because,

> Once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution.[78]

The court recognized the Fourth Amendment requirement as a critical constitutional protection of individual privacy and therefore expressly limited this foreign intelligence exception of the warrant requirement to instances in which the purpose of the search or wiretap was to obtain foreign intelligence information.[79] As discussed previously, Section 218 provides law enforcement officials with the opportunity to perform surveillance under FISA guidelines even though a central goal of the surveillance is to gather criminal investigation information. If courts follow their own precedent, terrorists could go unpunished because the evidence

---

[76] ACLU, *supra* note 61.

[77] *Id.*

[78] *Truong Dihn Hung*, 629 F.2d at 915. The relevant test is not conducting surveillance under FISA solely for foreign policy reasons because almost all foreign intelligence investigations are in part criminal investigations.

[79] *Id.* at 916.

obtained by the surveillance pertaining to their criminal activity would be suppressed in a criminal case.

The unconstitutional provisions of Title II will likely be overruled by some courts, thereby minimizing the USA PATRIOT ACT's effectiveness. Senator Patrick Leahy noted "some of these provisions will face difficult tests in the courts."[80] Even if the courts are lenient in the times closely following September 11, 2001, as time elapses the leniency will lessen, and provisions are more likely to be overruled.[81]

4. THE REMEDY

Section 218 does not further the goal of the USA PATRIOT ACT, to protect against terrorism. The pre-September 11th FISA provision respected constitutional civil liberties, while allowing law enforcement to gain intelligence information in order to protect the national security of the United States. Warrants under the pre-September 11th standard were not denied frequently. During the first 10 years of the FISA, the Foreign Intelligence Surveillance Court did not deny one government request out of over four thousand matters involving electronic surveillance that used assorted techniques directed at assorted types of targets in assorted circumstances.[82] Over the last decade, only three wiretap requests were denied from federal and state law enforcement.[83] From 1996 through 2000, authorities requested 4,275 FISA wiretaps and physical searches and no application was denied under the statute.[84] Also, the courts have never granted a suppression motion on FISA evidence.[85] The FISA provided our intelligence community with the authority to investigate a large variety or individuals and organizations, and to thereby defend against terrorism.[86]

Section 218 will not aid in the protection against terrorism since FISA warrant applications are rarely denied. Rather, it enables law enforcement officials to search or wiretap parties without having probable cause, with a goal to use that information in a criminal investigation. In other words, Section 218 enables the law enforcement to violate the Fourth Amendment. In addition, evidence of terrorist activity could be found inadmissible

---

[80] Jess Bravin, *House, Senate Move Closer on Counterterrorism Measures,* WALL ST. J., Oct. 15, 2001, at A26.

[81] See *Id.*

[82] Cinquegrana, *supra* note 17, at 815.

[83] THE AMERICAN CIVIL LIBERTIES UNION TEXAS, *Wiretapping: Why Is Congress Being Asked to Jettison Even the Most Basic Protections?, at* http://www.aclutx.org/projects/police/HomelandSecurity/wartimewiretapping.pdf.

[84] Cinquegrana, *supra* note 17, at 814.

[85] John Gibeaut, *Winds of Change*, 87 A.B.A. J. 32 (Nov. 2001).

[86] *Hearings, supra* note 8, at 30 (statement of Jerry Berman).

because of Fourth Amendment violations. To further the goal of the USA PATRIOT ACT, to protect against terrorism, Section 218 should be removed from Title II.

B. Pen Registration, Trap and Trace Devices

Prior to the USA PATRIOT ACT, the statutes that governed the use of pen registration and trap and trace devices were structured according to the understanding that the telephone was the predominate method of communication across a distance.[87] Pen registration surveillance devices allowed the government to capture the electronic or other impulses which identified the phone numbers dialed on outgoing telephone calls; trap and trace surveillance devices allowed the government to capture the electronic or other impulses which identified numbers of the incoming telephone calls.[88] The Supreme Court held that there is no constitutionally protected privacy interest in the numbers one dials to initiate a phone call.[89] This is because "neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[90]

Federal law enforcement officials conduct approximately ten times more pen register and trap and trace surveillance operations than they do wiretaps.[91] They use this form of surveillance frequently because courts require few things to grant pen registers and trap and trace orders. To obtain either court order, the law enforcement officer needs to attest that the information to be obtained is "relevant to an ongoing criminal investigation."[92] Upon the government official's attestation, the court "shall" issue the pen register or trap and trace device.[93] As long as the application contains an assertion that the information sought is relevant to the investigation, a court will authorize the installation of the pen register or trap and trace device and will not conduct an independent judicial inquiry

---

[87] Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VA. J. L. & TECH. 4, 2 (2001).

[88] 18 U.S.C. § 3127(3) (2000); 18 U.S.C. § 3127(4) (2000).

[89] Smith v. Maryland, 442 U.S. 735, 742 (1979).

[90] United States v. New York Telephone Co., 434 U.S. 159, 167 (1977).

[91] CENTER FOR DEMOCRACY AND TECHNOLOGY, *CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protection* (Apr. 4, 2000), *at* http://www.cdt.org/security/000404amending.shtml.

[92] 18 U.S.C. § 3123(a) (2001).

[93] *Id.*

into the veracity of the attested facts.[94] Thus, issuing a pen register or trap and trace device requires a low standard of proof, far below the probable cause standard.[95]

However, in order to have access to the contents of the telephone communication, the officer had to prove probable cause, that is, that a crime has occurred, is occurring, or will occur.[96] Title III of the federal wiretap statute governs the interception of the content of communications; content is defined as "any information concerning substance, purport, or meaning of that communication."[97] Unlike the low standard required to obtain a pen register or trap and trace device court order, the Supreme Court has held that the Fourth Amendment limitations on searches and seizures apply to the content of communications.[98] Therefore, Title III limits the access law enforcement officials have to obtain call content.[99]

Before September 11th, pen register and trap and trace laws had been written in a world of hard-wired telephones, not envisioning the electronic communication of today.[100] The pre-September 11th statutes' application to modern long distant communication, such as the internet, was unclear. Although court orders applied to Internet activity, the statutes did not specify the equivalent of the dialing information.[101] September 11th highlighted the inefficiency and potential harm resulting from this lack of clarity. The individuals who carried out the September 11th terrorist atrocity used email and the Internet to help complete the attack.[102] In fact, public accounts indicate that several of the terrorists received training on the Internet to prepare for the attack.[103] September 11th highlighted the deficiencies of old pen register and trap and trace laws and illustrated the

---

[94] In re Application of the United States, 846 F. Supp. 1555, 1558-59 (M.D. Fla. 1994); *see also*, United States v. Fregoso, 60 F. 3d 1314, 1320 (8th Cir. 1995) (stating that, "The judicial role in approving use of trap and trace devices is ministerial in nature.").

[95] 18 U.S.C.S. § 3123 (1993).

[96] 18 U.S.C.S. § 3122 (1993).

[97] 18 U.S.C. § 2510(8) (1996).

[98] CENTER FOR DEMOCRACY AND TECHNOLOGY, *supra* note 91.

[99] 18 U.S.C. § 2518(3) (1996). A law enforcement official may intercept the content of communications only when a court order is issued upon finding probable cause to believe that an individual is committing one of a list of specifically enumerated crimes, that communications concerning the specific offense will be obtained, and that the pertinent facility is used by the alleged offender commonly, or is used in connection to the offense.

[100] Walter S. Mossberg, *In Wake of Terrorism, It's Time for the Internet To Face the Real World*, WALL ST. J., Oct. 4, 2001, at B1.

[101] CENTER FOR DEMOCRACY AND TECHNOLOGY, *supra* note 91.

[102] Mossberg, *supra* note 100.

[103] *Id.*

need to keep up with technology. Section 216 updates the law to keep in-step with technology, but does so in an unconstitutional manner.

1. SECTION 216 OF THE USA PATRIOT ACT

In order to meet the needs of law enforcement investigations in a world of advanced technology, Section 216 extends access to Internet communications. Now, Section 216 gives law enforcement agents access to "dialing, addressing, routing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," once they have obtained pen register and trap and trace orders.[104] In addition to the outgoing dialed telephone numbers and the origin of the incoming telephone calls, pen registers and trap and trace orders now provide access to much more information contained in an electronic communication: the routing, addressing and signaling information of an electronic communication.[105] However, Section 216 never defines the terms dialing, routing, addressing, or signaling.[106] Without clear definitions of these terms, Section 216 does not clarify what information law enforcement officers can access. Therefore, it will be left up to the courts. For example, courts could interpret the term "routing" information to include a computer code transmitted that indicates from which part of the Internet a person was requesting information, including search terms used to locate, for example, books on certain subjects to be ordered from on-line bookstores.[107] Also, without further clarification, "addressing" information might include Uniform Resource Locators ("URLs") which could describe the contents of a specific library of information on the Internet.[108] The new definitions of pen registers and trap and trace devices expand the amount of information law enforcement officials can access in an unclear way, yet a way likely to increase the intrusiveness of these devices.[109]

---

[104] H.R. 3162 § 216(c)(2), (3).

[105] *Id.*

[106] AMERICAN CIVIL LIBERTIES UNION, *How Anti-Terrorism Bill Limits Judicial Oversight of Telephone and Internet Surveillance* [hereinafter Anti-Terrorism Bill], *at* http://www.aclu.org/congress/1102301g.html (last visited Oct. 7, 2002).

[107] Taylor, *supra* note 87, at 5. For example, the term routing could provide access to DATA: GET/booksearch/results.asp?WRD=prostate+cancer&userid=4MOT3. This clearly includes content of the communication.

[108] *Id.* at 6. For example, the term addressing could provide access to a File Transfer Protocol Address such as ftp://ftp.mentalhealth.com/depression/treatments.

[109] *Id.* at 5.

2. SECTION 216 IS UNCONSTITUTIONAL

The nature of pen registers and trap and trace devices heightens the risk of civil liberty abuse created by the ambiguity of the terms used in Section 216. As discussed above, a court order granting either a pen register or a trap and trace device can be easily obtained. Since pen register and trap and trace device statutes lack many of the privacy protections found in Title III wiretap law, they were narrowly tailored to provide access to only the information not protected by the Fourth Amendment, the numbers one dials to initiate a phone call.

However, the definition of a pen register and a trap and trace device in Section 216 alters the intent of the old laws by allowing collection of information outside of identifying the origin device or the destination device of a communication.[110] Section 216 provides a pathway to the content of communications without having first developed probable cause. If the courts interpret the terms broadly, pen registers and trap and trace devices can provide access to contents of communications, thereby violating the Fourth Amendment of the Constitution.

3. SECTION 216 IS INEFFECTIVE

In an effort to counteract the accusation of allowing unconstitutional access to information, Section 216 states that the information gained from the dialing, routing, addressing or signaling sources "shall not include the contents of any communication."[111] However, this cannot be true due to the nature of the Internet. The numbers dialed to and from a telephone are not exclusively linked to the content of those communications, but are easily separated from the content of those calls.[112] In contrast, the contents of an email cannot be easily separated from undefined dialing, routing, addressing or signaling information.[113] Email communication travels in small packets, and someone must separate the content of a communication from its address.[114] Many Internet service providers ("ISPs") are not capable of discriminating between communications to isolate the specific types of information a pen register or trap and trace court order would authorize.[115]

---

[110] *Id.*

[111] H.R. 3162 § 216 (c)(2), (3).

[112] Anti-Terrorism Bill, *supra* note 106. After a telephone call is made, that part of the circuit switch network is dedicated only to that single connection. Taylor, *supra* note 87.

[113] *Id.*.

[114] *Id.*

[115] Taylor, *supra* note 87.

The FBI proposes as a solution that it obtain the entire message, and then be trusted to separate the information to which it is entitled by a pen register or trap and trace device from the content of the communication.[116] The FBI developed a computer program, Carnivore, which enables the interception and collection of only the communications allowed by the court order.[117] However, use of this program is left to the discretion of the FBI. Although the traditional pen register and trap and trace device law was self-regulating, when the court order grants access to routing, addressing, and signaling information, self regulation is no longer practical.[118] Under the traditional statutes, law enforcement officers could not reveal the content of communications because they only had access to the numbers dialed.[119] However, Section 216 provides the opportunity to willfully intrude on legitimately held privacy because the content of the call can be accessed. Making the FBI its own watch dog creates a situation ripe for abuse and therefore should not be allowed.

The FBI has abused its powers in the past. The FBI has investigated people because of ethnic background or political viewpoint, both of which unjustly invade the sacred American right of individual privacy. For example, the FBI conducted the COINTERLPRO investigation to spy upon and disrupt the anti-Vietnam War and pro-civil rights movements in the late 1960s and early 1970s.[120] Even during the 1980s, the FBI investigated the Committee In Solidarity With The People of El Salvador because this committee's members opposed the US policy of aiding repressive regimes in Central America (although this speech is traditionally protected by the First Amendment).[121]

The risk of abuse is extenuated by a report presented to the Federal Communications Commission ("FCC") that concluded that Carnivore presented several problems regarding its ability to filter information in packet-based networks such as the internet.[122] This report ultimately

---

[116] Anti-Terrorism Bill, *supra* note 106.

[117] Taylor, *supra* note 87.

[118] *Id.* at 7.

[119] *Id.*

[120] ACLU, *supra* note 61.

[121] *Id.*

[122] *See* JOINT EXPERTS, COMMITTEE TR 45, TELECOMMUNICATIONS INDUSTRY ASSOCIATION, REPORT TO THE FEDERAL COMMUNICATIONS COMMISSION ON SURVEILLANCE OF PACKET-MODE TECHNOLOGIES 12-13 (Sept. 29, 2000), *available at* http://www.tiaonline.org/policy/filings/JEM_Rpt_Final_092900.pdf. Carnivore has not yet proven effective in situations where the target's communications are part of a high bandwidth transmission. Second, many aspects of Carnivore are still untested such as certification or testing of the product and uncertainty about whether the filter produces information that is coextensive with call identifying information and who establishes the criteria for separation.

concludes that "there is no reliable method for determining the Pen Register and Trap and Trace information when monitoring a packet stream."[123] Therefore, the FBI cannot be allowed to self regulate the separation of court authorized information traveling over the Internet.

Section 216 does not prevent access to the content of communications by simply forbidding it. The nature of the Internet combined with the ambiguity of the terms routing, addressing and signaling information ensure content will be viewed. If courts find that pen registers and trap and trace devices cannot constitutionally reveal content of the communications, Section 216 will be ineffective in protecting against terrorism. Any incriminating evidence will be inadmissible. On the other hand, if courts admit evidence resulting from content obtained by a pen register or trap and trace device, the Fourth Amendment of the Constitution will be violated.

4. THE REMEDY

An update in the pen registration and trap and trace law was needed to protect against the dangers presented with advancing technology. However, Section 216 needs tighter language to safeguard against the unconstitutional viewing of the content of Internet activity. Records of the sites a person visits on the Internet are as equally deserving of privacy as records documenting hotel stays, car rentals and other real world activities.[124] Section 216 should be amended to abide by the Constitution while keeping in step with technology.

Section 216 should define pen registers as "dialing, routing, addressing or signaling information that identifies the destination of a wire or electronic communication transmitted by telephone line or other subscriber facility to which such device or process is attached or applied."[125] And the definition of trap and trace devices should read "a device or process that captures the dialing, routing, addressing or signaling information that identifies the originating instrument or device from which a wire or electronic communication was transmitted."[126] Section 216 should make it clear that a court order authorizing either surveillance device does not include the interception of search terms, URLs that identify specific documents, files, or web pages, or other transactional information.[127] If Section 216 is not amended, it violates the Constitution by providing access to the content of communications without having probable cause and fails to accomplish its goal of prohibiting access to that content.

---

[123] *Id.* at 59.

[124] Mossberg, *supra* note 100.

[125] CENTER FOR DEMOCRACY AND TECHNOLOGY, *supra* note 91.

[126] *Id.*

[127] *Id.*

C. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

A conventional wiretap can only be placed on a specifically designated telephone line at a specific location, which has been specified in the wiretap application.[128] If the suspect changes telephones, the law enforcement officials must reapply for a wiretap order for the other phone location.[129] Before granting a conventional wiretap, courts require that the applicant prove probable cause that the place from where the communications are to be intercepted is being used for criminal activity.[130]

As technology advanced, wiretapping requirements needed to be changed to remain effective. In 1986 roving wiretaps were created which allow law enforcement officials to place a wiretap on any telephone line from any location that a suspect uses.[131] Courts do not require probable cause that the place of the communication is being used for criminal activity to grant a roving wiretap. Instead, prior to the 1998 amendment, courts would require law enforcement officials to demonstrate that the suspect was purposely attempting to evade conventional wiretaps.[132] All federal courts that addressed the constitutionality of the original roving wiretap statute found it constitutional.[133] In each of the cases, the court found the original roving wiretap statute constitutional because of the statute's requirement to show that the target attempted to thwart surveillance.[134]

In 1998, Congress amended the roving wiretap act to require law enforcement officials only to demonstrate that a suspect's conduct *could have the affect* of thwarting surveillance, no longer requiring that the

---

[128] 18 U.S.C. § 2518(1) (2000) [hereinafter Wiretap Law].

[129] Bryan R. Faller, *The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better*, 60 OHIO STATE L. J. 2093, 2094 (1999).

[130] Wiretap Law, *supra* note 128.

[131] 18 U.S.C. § 2518(11)(b) (1994), *amended by* Pub. L. No. 105-272, 604, 112 Stat. 2396, 2413 (1998). This paper will use the phase "original roving wiretap statute" to refer to the original law enacted in 1986, and the "1998 amendment" to refer to the roving wiretap statute after 1998.

[132] 18 U.S.C. § 2518(11)(b) (1996) ("The applicant makes a showing of a purpose on the part of [the target] to thwart interception by changing facilities.").

[133] Faller, *supra* note 129, at 2113. *See, e.g.*, United States v. Gaytan, 74 F3d 545, 553 (5th Cir. 1996); United States v. Silberman, 732 F. Supp. 1057, 1063 (S.D. Cal. 1990); United States v. Parks, No. 95 CR. 510, 1997 WL 136761, at *18 (N.D. Ill. Mar. 24, 1997).

[134] *Id.*

suspect's conduct purposely evaded surveillance.[135] As amended, the roving wiretap statute endangers personal privacy and violates the particularity requirement of the Fourth Amendment.[136] In some circumstances, rather than requiring the exact location of the place to be searched, courts require the law enforcement officers to provide *other information* that sufficiently defines the place to be searched in order to meet the particularity requirement.[137] The original statute's requirement that a suspect purposely try to evade detection satisfies this 'other information' requirement.[138] However, the 1998 amendment's requirement that the suspect's behavior could have the affect of thwarting surveillance does not. The amendment allows law enforcement officers to obtain a roving wiretap based on everyday occurrences.[139] The amendment's standard can be met too easily to properly limit the intrusive nature of roving wiretaps. The 1998 amendment is unconstitutional, and the same civil liberties violation should not be repeated in the USA PATRIOT ACT.

1. SECTION 206 OF THE USA PATRIOT ACT

Section 206 states that roving wiretaps will be applicable to FISA "in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person."[140] It extends the 1998 amendment standards to FISA, not the standards of the original roving wiretap statute. A roving wiretap will be granted in a FISA investigation based on everyday behavior. Each phone in a phone bank could be wiretapped if the FBI got a report that the target of a FISA investigation simply used one of those phones once. The private conversations of innumerable innocent Americans with absolutely no connection to the investigation would be subject to government scrutiny.[141]

---

[135] 18 U.S.C. § 2518(11)(b) (1994), *amended by* Public Law Number 105-272, 604, 112 Stat. 2396, 2413 (1998) (emphasis added).

[136] Faller, *supra* note 129, at 2096. Although the particularity requirement is not easily satisfied by warrants for roving wiretaps, the Fourth Amendment has been interpreted to conform to changing technology. *Id.* at 2115.

[137] *Id.* at 2116 (emphasis added).

[138] *See Id.*

[139] *Id.* at 2113.

[140] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [hereinafter USA Patriot Act], Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001).

[141] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10576, (statement of Mr. Feingold).

2. SECTION 206 IS UNCONSTITUTIONAL

Section 206 is unconstitutional because it extends the unconstitutional 1998 amendment of the original roving wiretap statute to FISA. By granting a roving wiretap based only on the claim that the actions of the target may have the effect of thwarting his or her identification, falls short of meeting the particularity requirement of the Fourth Amendment.[142] In practice, courts may grant roving wiretaps for virtually any FISA target. When roving wiretaps are used in intelligence surveillance circumstances, not criminal, they pose a greater threat to privacy because intelligence wiretaps are authorized secretly without showing any probable cause of a crime.[143] Individuals under no suspicion are at risk of having their privacy violated.

In addition, Section 206 does not require that law enforcement agents ascertain that the target is actually using the communication device.[144] The original roving wiretap statute required that, before a particular telephone line could be tapped, the law enforcement agent needed to ascertain that the target was actually using the line, although this was not required by the 1998 amendment.[145] That protection helped to minimize the privacy invasion of individuals unrelated to the investigation.[146] Section 216 allows the FBI to go from computer to computer, phone to phone, without any certainty that the device is used by the suspected terrorist.

3. SECTION 206 IS EFFECTIVE

Section 206 violates the Constitution, yet will probably not be overruled by courts. Taking into account that the 1998 amendment to the roving wiretap statute has not been ruled unconstitutional by any courts yet, courts are not likely to find Section 206 unconstitutional and suppress any information gained through the surveillance.[147] Therefore, if information gained through a roving wiretap granted under the loose requirements of Section 206 helps to prevent a terrorist action, the section may be effective in protecting against terrorism. However, the provisions of Title II should

---

[142] *See* Bryan R. Faller, *supra* note 129, at 2116.

[143] Anti-Terrorism Bill, *supra* note 106.

[144] *See* USA Patriot Act, *supra* note 140, at § 206.

[145] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10575-6 (statement of Mr. Feingold).

[146] *Id.*

[147] Due to the more severe infringement of civil liberties when conducting FISA surveillance, the courts could distinguish roving wiretaps when applied to FISA and find § 206 unconstitutional. If so, § 206 would no longer effectively protect against terrorism because the evidence gathered would be inadmissible.

be structured to both effectively protect against terrorism, and respect the civil liberties granted by the Constitution.

4. THE REMEDY

Roving wiretap authority is already available for criminal investigations under Title III. To protect against terrorism by keeping up with advancing technology, it is appropriate to apply roving wiretaps to the FISA. However, Section 206 should be modeled after the 1986 statute of roving wiretaps. It should allow roving wiretaps to be used in FISA investigations, "in circumstances where the court finds that the actions of the target of the application demonstrate that the suspect was purposely trying to evade conventional wiretaps."[148] The original roving wiretap statute contained key safeguards that minimized the possible misuse of authority to eavesdrop on individuals whom are not a part of the investigation. Also, the original law required that the actual interception could not begin until the suspect begins or shows an intention to begin a conversation. Roving wiretaps should only be granted under FISA if the law enforcement officials meet this standard because of the heightened risks presented when applied to intelligence surveillance circumstances.

The original roving wiretap statute served law enforcement effectively in conducting surveillance on very sophisticated criminal organizations, including drug importation organizations and the mafia.[149] When Congress passed the 1998 amendment, it did so covertly. The 1998 roving wiretap amendment was not included in the initial versions of the Intelligence Authorization Bills that were approved by the House of Representatives and the Senate.[150] Rather, the amendment was added during a conference, absent hearings and debate.[151] The Explanatory Statement of the managers of the conference did not explain why the amendment was needed.[152] Thus, there is no persuasive reason justifying the 1998 amendment, yet it violates the constitution. Section 206 should not be modeled after this amendment.

---

[148] *See* 18 U.S.C. § 2518(11)(b)(ii) (1994).

[149] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10576 (statement of Mr. Feingold). A provision identical to that of the 1998 amendment failed to be passed after much debate in response to the 1996 Anti-Terrorism Act. *See also* Teresa Kolb Weil, *Roving Wiretaps: For Your Ears Only*, 45 LOY. L. REV. 745, 746. (1999).

[150] *See* Kolb Weil, *supra* note 149.

[151] *See id.* "When a piece of legislation returns from conference it is no longer subject to amendment.. Congressional rules specify that the full bodies must either pass the entire bill or turn it down." *Id.* at 746 n. 8.

[152] Faller, *supra* note 129, at 2105.

D. Authority for Delaying Notice

The Fourth Amendment of the United States Constitution requires that the government obtain a warrant and give notice to the target before conducting the search to protect against unreasonable search and seizures.[153] A warrant is required to minimize the privacy invasion of a search by allowing a neutral and detached third party to determine its scope.[154] However, the privacy protection granted by the warrant greatly lessens if the target does not receive notice of the search because the agent cannot be held accountable to the terms of the warrant. If the secret search warrant specifies a particular place or item to be searched, there is little incentive to abide by the terms of the warrant because the target does not know those terms. Elimination of notice deprives the target of the opportunity to challenge the deficiencies in the warrant, thereby denying the target the right to assert his or her Fourth Amendment rights.[155]

The Federal Rules of Criminal Procedure prohibit secret searches for physical evidence by requiring that the law enforcement officials conducting the search "leave a copy and receipt at the place from which the property was taken."[156] Title 18 of the United States Code loosens this requirement by allowing for the delayed notice of searches of oral or wire communications.[157] Prior to the USA PATRIOT ACT, if a court was to grant delayed notice, the law enforcement officer was required to show that if notice was given, an individual's physical safety would be endangered, someone would flee prosecution, evidence would be tampered with, potential witnesses would be intimidated, or an investigation would be jeopardized.[158] The circumstances that justified delayed notice of a search prior to September 11th are clearly specified, limited, and largely exigent circumstances.

---

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

[154] *See* AMERICAN CIVIL LIBERTIES UNION, *How the Anti-Terrorism Bill Expands Law Enforcement "Sneak and Peek" Warrants,* Oct. 23, 2001 [hereinafter AMERICAN CIVIL LIBERTIES UNION], *at* http://www.aclu.org/congress/1102301b.html.

[155] Letter from the American Civil Liberties Union to Members of Congress concerning Sneak and Peek Search Warrants on Anti-Terrorism Legislation (Oct. 19, 2001) [hereinafter ACLU Letter], *at* http://archive.aclu.org/congress/l101901a.html.

[156] FED. R. CRIM. PROC. 41(d).

[157] ACLU Letter, *supra* note 155. However, the criminal code never permitted secret searches for criminal evidence. Although there is no legal authority for such actions, the FBI sometimes conducted covert searches. Most courts, including the Supreme Court of the United States, have not ruled on the constitutionality of this practice. Case law is limited and confused.

[158] AMERICAN CIVIL LIBERTIES UNION, *supra* note 154.

1. SECTION 213 OF THE USA PATRIOT ACT

Section 213 broadens the circumstances in which notice of any court order or warrant can be delayed beyond instances of exigent circumstances. It allows delayed notice of the issuance of any court order or warrant if three easy qualifications are met.[159] First, the court must find that providing immediate notification of the execution of the warrant *may have an adverse result.*[160] Second, the warrant can allow seizure of the item where the court finds *reasonable necessity* for the seizure.[161] Third, although the warrant must require that notice be given within a reasonable period, the *court can extend this period* for good cause.[162] Law enforcement agents now must only show that immediate notification of the warrant may cause an adverse result, a very easy standard to meet. Section 213 greatly expands the government's authority to conduct secret searches. Law enforcement agents can now enter a person's home or business and conduct a search without the person realizing that a search occurred.[163] This section transforms extremely limited authority into an authority available in any kind of search, physical or electronic, and in any kind of criminal case.

2. SECTION 213 IS UNCONSTITUTIONAL

Section 213 violates the Fourth Amendment of the Constitution by allowing for delayed notice of searches and seizures in unclear, broad, non-exigent circumstances. The Fourth Amendment notice requirement is disregarded without sufficient justification. As discussed previously, prior to the USA PATRIOT ACT, a delayed notice was only permitted if an individual's physical safety would be endangered, someone would flee prosecution, evidence would be tampered with, potential witnesses would be intimidated, or an investigation would be jeopardized. Fundamentally,

---

[159] USA Patriot Act of 2001, H.R. 3162 108th Cong. § 213 (b) (1)&(2)&(3) (2001) ("(1)[T]he court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result; (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication, or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and (3) the warrant provides for the giving of such notice within a reasonable period of it execution, which period may thereafter be extended by the court for good cause shown.").

[160] H.R. 3162 § 213(b)(1) (emphasis added).

[161] H.R. 3162 § 213(b)(2) (emphasis added).

[162] H.R. 3162 § 213(b)(3) (emphasis added).

[163] ACLU Letter, *supra* note 155.

the Fourth Amendment only prohibits unreasonable searches and seizures. It is reasonable in certain circumstances to sacrifice the target's right to notice of a search or seizure. However, Section 213 extends the circumstances that allow for delayed notice too broadly. Everyday behavior of a target and frequent circumstances could be interpreted as potentially resulting in an adverse outcome if immediate notification were given, the main requirement of Section 213.

3. SECTION 213 IS INEFFECTIVE

Section 213 is not necessary to accomplish the goal of protecting against terrorism because delayed notice was already sufficiently available. If notice would jeopardize an investigation, notice would be delayed. If notice would endanger physical safety, it would be delayed. Extending the circumstances in which law enforcement officials can withhold notice does not prevent terrorism because, if essential to the investigation, it could otherwise be granted.

4. THE REMEDY

Section 213 does not further the goal of protecting against terrorism, yet it violates the Fourth Amendment of the Constitution. Accordingly, it should be deleted from Title II of the USA PATRIOT ACT. Law enforcement officials already had limited ability to delay providing the notice of a search to the target in explicit, narrow, largely exigent circumstances. An official could delay notice in situations where, if notice were given, an individual's physical safety would be endangered, someone would flee prosecution, evidence would be tampered with, potential witnesses intimidated, or an investigation jeopardized. This list of circumstances sufficiently aids the fight against terrorism. Delaying notice of the search to the target in any other circumstances violates his or her civil liberties and those of innocent people more than it aids in the protection against terrorism. Therefore, Section 213 should be removed from Title II.

E. The Sharing of Information

Section 203 grants new authority to share criminal investigative information. Many officials stated that the coordination and consolidation of information from agencies such as the FBI and CIA are needed to increase national security.[164] However, an improved method of sharing

[164] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10578 (statement of Mr. Leahy).

information between the FBI and CIA, governmental agencies, does not mean that the type of information shared needs to be broadened.

Current law allows the sharing of confidential criminal justice information, but with close court supervision. The Federal Rules of Criminal Procedure state that information shared in the grand jury may be disclosed only to a government attorney, assisting governmental personnel, and another grand jury.[165] Only the court can authorize further disclosure.[166] Last year, the Justice Department stated that "law enforcement agencies have authority under current law to share Title III information regarding terrorism with intelligence agencies when the information is of overriding importance to the national security."[167]

1. SECTION 203 OF THE USA PATRIOT ACT

Section 203(a) allows grand jury information to be shared "when matters involve foreign intelligence or counterintelligence . . . or foreign intelligence information . . . to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of official duties."[168] Section 203(b) extends the authority to share electronic, wire and oral interception information in the same manner.[169] Section 203 redefines "foreign intelligence information," to permit more liberal sharing of information about American people.[170] Foreign intelligence information is defined as information that relates to the ability of the United States to protect against an actual or potential attack, sabotage or clandestine intelligence activity.[171] This definition is so broad that practically any behavior could fit into the definition if a law enforcement officer or judge desired.[172]

---

[165] FED. R. CRIM. PROC. 6(e).

[166] *Id.*

[167] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10555 (statement of Mr. Feingold). Taken from a Letter from Robert Raben, Assistant Attorney General (Sept. 28, 2000).

[168] *See* USA Patriot Act, *supra* note 140, at § 203(a)(1)(c)(i)(v).

[169] USA Patriot Act, *supra* note 140, at § 203(b)(1).

[170] AMERICAN CIVIL LIBERTIES UNION, *How the Anti-Terrorism Bill Puts The CIA Back Into Business of Spying on Americans,* Oct. 23, 2001 [hereinafter *Business of Spying*], *at* http://archive.aclu.org/congress/l102301j.html.

[171] USA Patriot Act, *supra* note 140, at § 203(a)(1)(iv); (6)(2)(19); (d)(2).

[172] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10556 (statement of Mr. Leahy).

2. SECTION 203 IS UNCONSTITUTIONAL

Historically, information sharing between the CIA and FBI has enabled the CIA to spy on the American public, violating Constitutional civil liberties. The CIA illegally investigated Americans until the mid-1970s.[173] The CIA spied on as many as seven thousand Americans in an intelligence operation entitled CHAOS, regardless of the fact that the CIA's statutory charter prohibited the CIA from engaging in internal security functions.[174] This operation involved extensive information sharing between the FBI and other CIA agencies concerning people who opposed the Vietnam War, student activists, and black nationalists.[175] For example, the FBI shared all of its reports on the American peace movement, totaling over 1,000 a month by June of 1970.[176]

A Congressional report, the Church Committee Report, revealed the tremendous extent that other agencies shared simple, passive information with the CIA, essentially authorizing spying and data collection on lawful American political activity traditionally protected by the Constitution.[177] Upon the CIA's subtle request for a particular type of information concerning American individuals and groups, other federal and local agencies were persuaded to covertly spy on citizens.[178] The Church Reports referred to this type of action as "a step toward the dangers of a domestic secret police against which the prohibition of the charter sought to guard."[179] After the Church Reports exposed these abuses, the CIA's domestic surveillance activities were greatly limited.[180] The USA PATRIOT ACT eliminates the safeguards the Church Report identified, putting the CIA in a position to spy on American people, violating their Fourth Amendment rights.[181]

Section 203 disregards the safeguards established by the Church Committee Reports. Leaks from the FBI can irreparably damage innocent people's reputation, and can frustrate investigations by alerting suspects to flee or destroy material. The bill does not provide for judicial supervision of the new authorization for dissemination of grand jury information

---

[173] *Business of Spying, supra* note 170.

[174] *Id.*

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] *See id.*

throughout the executive branch.[182] The information that can be shared about the suspect is not limited.[183]

3. SECTION 203 IS INEFFECTIVE

Granting increased powers to share information will only effectively protect against terrorism if such information is successfully communicated among governmental agencies. Section 203 fails to address the specifics of how information will be communicated. To be discussed in greater detail in section IV, the FBI neither processed the information it gains effectively, nor communicates significant details. Until these internal organizational problems are improved in each governmental agency, increasing the amount of information that will be share is ineffective.

4. THE REMEDY

Limited sharing of information is appropriate, but strict safeguards should limit the information communicated.[184] Sharing information poses a real threat to the privacy of American citizens. Section 203 should have included a narrower definition of foreign intelligence information to ensure that the information communicated between agencies only applied to circumstances of national security threats.[185] If there are specific laws that the Administration believes impede the necessary sharing of information on terrorism and foreign intelligence, those problems should be addressed through legislation narrowly targeted to those statutes.[186]

Terrorism is best protected against if pertinent information regarding terrorism is shared. The CIA and FBI already had this power.[187] However, history indicates that there must be strict limits on what can be shared. Otherwise, the CIA could be put in a position to spy on Americans. Rather than increasing the amount and broadening the type of information that can be shared, practical mechanisms should be developed that facilitate government agencies' ability to communicate. As will be discussed in Section IV, organizational and managerial skills should be developed to

---

[182] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10556 (statement of Mr. Leahy).

[183] *Business of Spying, supra* note 170.

[184] H.R. 3162, 107th Cong. § 203(b) (2001) (granting law enforcement agents the authority to share electronic, wire, and oral interception information).

[185] *Id.*

[186] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10556 (statement of Mr. Leahy).

[187] *Id.*

insure that information is shared, rather than a new power extending the amount of what is allowed to be shared.

IV. EFFECTIVE ALTERNATIVES: THE MANAGERIAL SOLUTION

The September 11th atrocities were not committed by an enemy who sought territory, resources, or material gain, but rather by enemies of the beliefs and values of the United States' people, specifically our beliefs in freedom, as pointed out by Attorney General Ashcroft.[188] He went on to promise, "we will not now allow our values to become victims."[189] However, as discussed in the previous section, Title II's extension of surveillance powers victimizes American values. Increasing surveillance powers may comfort and reassure scared American citizens, but does not increase their protection against terrorism. Instead of hastily increasing surveillance powers, the government should have identified barriers preventing effective protection against terrorism, such as: internal weaknesses of the FBI, inabilities to digest and communicate information, misguided drafting procedures, and ineffective agency coordination.

A. Improving the FBI Internally

September 11, 2001, represents one of the most extensive intelligence failures that the world has ever seen.[190] For as many as five years, nineteen people worked on a complex terrorist operation to crash multiple planes into several targets.[191] The amount of planning necessary to complete this act suggests that the agency in charge of domestic surveillance, the FBI, is to blame.[192] However, this is an incorrect, short-sighted presumption. The FBI's use of electronic surveillance procedures is not to be blamed, because when a terrorist group is cautious, close-knit, and never purchases large amounts of illegal material, wiretapping and other law enforcement techniques are not effective preventive mechanisms.[193] The increased surveillance powers granted by Title II would not have stopped this attack. Although September 11th demonstrated that the United States intelligence gathering system must be improved, that is not accomplished by granting overly broad, unconstitutional powers. The existing agencies need internal improvement.

---

[188] Attorney General John Ashcroft, *supra* note 57.

[189] *Id.*

[190] *Testing Intelligence*, THE ECONOMIST, Oct. 6, 2001, at 31-32.

[191] *Id.*

[192] *Id.* at 31.

[193] *Id.*

Experts now suggest that the FBI make five changes: hire more spies; change the hiring practices of the FBI; improve the level of professionalism within the bureau; change its priorities; and improve coordination within the FBI.[194] A report for Congress emphasized that the United States needs to strengthen its human intelligence collection capacity in the form of spies, rather than intelligence gathering by satellite or other technical means.[195] These suggestions do not require adding electronic surveillance powers that place civil liberties at high risk, but rather strengthen the FBI's internal functioning. Improving the organization, management and resources of the FBI enable it to protect against terrorism more effectively than broad, unconstitutional increases in surveillance powers.

A General Accounting Office ("GAO") report to Congressional Committees, scheduled for release in September prior to the September 11th atrocities, summarized federal efforts to combat terrorism prior to these events.[196] This report argued that the overall leadership of the counter-terrorism forces and coordination of responsibilities needed to be centralized and clarified.[197] The majority of recommendations involve the functioning of already created organizations, not the granting of new powers.[198] As stated in the Report of the National Commission on Terrorism, in many situations law enforcement agents are unsure as to when the particulars of a given case merit the broader authority to be invoked.[199] This lack of clarity contributes to a risk-adverse culture that causes some agents to refrain from taking prompt action against suspected terrorists.[200] Even though the Oklahoma City bombing officials attempted to clarify the circumstances that would merit investigation, there is still considerable confusion among FBI field agents about the application of guidelines.[201] Guidelines should specify what facts and circumstances warrant the

---

[194] *Id.* at 31-32.

[195] Congressional Research Service Report for Congress, *Terrorist Attack on USS Cole: Background and Issues for Congress* 4 (Jan. 30, 2001).

[196] U.S. General Accounting Office, *supra* note 9, at 17. These efforts include: (1)Designate a single focal point with responsibility and authority for all critical functions necessary to provide all leadership and coordination of federal programs to combat terrorism; (2)Direct the focal point to develop a formal process to evaluate interagency lessons learned from major federal exercises to combat terrorism; (3)Consolidate selected Department of Justice and Federal Bureau of Investigation assistance programs to state and local governments into the Federal Emergency Management Agency.

[197] *See id.* at 31.

[198] *See id.* at 17.

[199] Richelson & Evans, *supra* note 3, at 9.

[200] *Id.* at 10.

[201] *Id.*

opening of a preliminary inquiry or full investigation, enabling FBI agents to take prompt action against terrorists.[202]

B. Digesting and Communicating Information

United States intelligence and law enforcement communities are not able to prioritize, translate, and understand all of the information to which they have access in a timely fashion.[203] The ability to quickly locate every pointed file, out of hundreds, that could lead to the prevention of a terrorist attack is extremely difficult.[204] In order to determine what information is relevant, large amounts of surveillance information must be processed, which can involve decrypting, translating, and deciphering code words used in a conversation.[205] Until each communication is in English, it is impossible to tell what is relevant.[206] Essential to an effective counter-terrorism program, the law enforcement agencies must be able to make use of the information collected.[207] The Report of the National Commission on Terrorism found that the law enforcement agencies were not making use of the information they collected during terrorism investigations, nor distributing that information effectively to analysts and policy makers.[208] The FBI would benefit from enhanced data storage, retrieval systems, counter encryption equipment, and linguists to translate raw data into useful information.[209]

Adding to the overload of information requiring analysis, the broader surveillance powers granted by Title II of the USA PATRIOT ACT will generate enormous amounts of data. Billions of telephone calls, e-mails, and wireless transmissions occur everyday, each an opportunity to use surveillance to catch terrorists.[210] Sifting out the significant communications that warrant a closer look is the difficult part.[211] Often the capacity to produce large amounts of data is not matched by sufficient tools

---

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] *Id.* at 15.

[209] *Id* at 14.

[210] Nicole Ridgway, *We Hear You – Echelon has its ears to the world's villains*, FORBES, Oct. 15, 2001, at 48.

[211] *Id.*

to interpret the information.[212] Justice Department officials expressed doubt in the FBI's ability to handle massive amounts of information generated by current terrorism investigations.[213]

After the significant facts are gathered, agencies must be organized well to be effective. Even in the aftermath of September 11th, when security concerns were extremely high, evidence indicated that the FBI was not successfully transmitting urgent warnings from Washington to local police.[214] For example, in a region where crop dusting is common, a chief law enforcement official said, "we haven't heard anything about the delays on crop dusting or about explosives or the list of people they are looking for."[215] Another example of poor organization failing to utilize information effectively is when the execution of Oklahoma City bomber, Timothy McVeigh, had to be delayed when FBI field offices around the country discovered that hundreds of documents that were supposed to have been turned over during the McVeigh trial were never given to defense lawyers.[216] "The law enforcement community is neither fully exploiting the growing amount of information it collects during the course of terrorism investigations nor distributing that information effectively to analysts and policymakers."[217] If law enforcement is not able to make use of the information gained using powers granted by Title II of the USA PATRIOT ACT, the newly granted surveillance powers do not protect against terrorism, yet they do violate the Constitution.

C. Drafting Well Thought-out Legislation

Many lawmakers voted for the USA PATRIOT ACT despite concerns that many provisions of Title II were overly broad.[218] Senator Patrick Leahy said that he yielded "to preserve national unity in a time of crisis," not because he supported the content of the legislation.[219] Although several members of Congress saw value in the proposed amendments that lessened the provisions' civil liberty violations, they withheld their support in order

---

[212] Ted Bridis & Gary Fields, *Would the FBI Know What to Do With its New Snooping Powers?*, WALL STREET. J., Sept. 26, 2001, at A1.

[213] *Id.*

[214] *See Id.*

[215] *Id.*

[216] *Id* at A6.

[217] Richelson & Evans, *supra* note 3 at 15.

[218] *See* Jess Bravin, *House, Senate Move Closer on Counterterrorism Measures*, WALL STREET. J., Oct. 15, 2001, at A26.

[219] *Id.*

to pass legislation immediately.[220] In addition, the anthrax scare spurred public pressure to produce anti-terrorist legislation.[221]

Congress completed the legislation process with undue haste.[222] The House voted on a 175 page bill that had been written only the night before by Congressmen who largely lacked the time to draft legislation properly.[223] Congressman Barr questioned whether the Justice Department was seeking "to take advantage of what is obviously an emergency situation."[224] The department, he said, "has sought many of these authorities on other occasions and has been unsuccessful in obtaining them."[225] The enormous public pressure to act quickly to fight against terrorism hindered much of the effort to minimize or prevent the overly-expansive new powers in the Act.[226] By rushing the legislation, ideas that might have flowed from careful examination of the problems law enforcement faced before September 11th were prevented from developing.

D. Creating a Manageable Chain of Command

On October 8, 2001, the President of the United States created the office of Homeland Security in an attempt to improve the coordination of governmental agencies.[227] Its mission is "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."[228] The President specified that, "the functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[229] The creation of the Office of Homeland Security resembles the type of internal organization that will effectively protect against terrorism without violating Americans'

---

[220] *Debate: Uniting and Strengthening America Act, supra* note 6, at S10577-8, S10588 (stated by many).

[221] *The Congress in Battle*, THE ECONOMIST, Oct. 20, 2001, at 31.

[222] *Id.*

[223] *Id.*

[224] Greg Miller & Edmund Sandaers, *Lawmakers Say Bill Raises Concerns for Civil Liberties*, L.A. TIMES, Sept. 25, 2001, at A1.

[225] *Id.*

[226] Amy Borrus, *When Right and Left See Eye to Eye*, BUSINESS WEEK, Nov. 5, 2001, at 88.

[227] *Executive Order establishing Office of Homeland Security and Homeland Security Council*, Oct. 8, 2001, *available at:* http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html (last visited Oct 1, 2002)

[228] *Id.*

[229] *Id.*

civil liberties. However, its creation satisfies just one aspect of the needed reorganization and improved management of governmental agencies.

Tom Ridge, the head of the Office of Homeland Security, bears the enormous responsibility of coordinating four dozen agencies and bureaucracies that now need to work together to secure the nation's borders, protect nuclear power plants, share intelligence, secure public facilities and fight bioterrorism.[230] In order for Tom Ridge and the Office of Homeland Security to be effective, the agencies and bureaucracies which he coordinates must each possess effective internal management and communication. However, many of these agencies and bureaucracies do not. One of the agencies overseen by the Office of Homeland Security is the FBI.[231] As previously discussed, the FBI does not digest and communicate information well,[232] and has inadequate internal organization.[233] The FBI fails to protect against terrorism sufficiently due to these inadequacies. To maximize protection against terrorism and minimize civil liberty violations, each agency and bureaucracy needs to improve its organization and communication.

V. CONCLUSION

September 11th illustrated that the United States needed to improve its ability to protect the country from terrorism. In response, the government hastily drafted legislation, the USA PATRIOT ACT. Five provisions of Title II, Enhanced Surveillance Procedures, of the USA PATRIOT ACT, either violated the Constitution of the United States, did not effectively protect against terrorism, or both. Rather than immediately granting broader surveillance procedures that impede civil liberties, the government should have first analyzed the barriers inhibiting effective use of existing policies that protect against terrorism. If done, the government would have detected internal weaknesses of the FBI, the inability of agencies to digest and communicate information, misguided drafting procedures, and ineffective agency coordination. These weaknesses need to be addressed today and strengthened to protect the United States against terrorism. Also, the five provisions of Title II of the USA PATRIOT ACT need to be amended in ways to minimize civil liberty violations while maximizing effectiveness to protect against terrorism.

---

[230] Alison Mitchell, *A Nation Challenged: The Security Chief; Disputes Erupt on Ridge's Needs for His Job*, N.Y. TIMES, Nov. 4, 2001, at B7.

[231] *See id.* (chart depicting breadth of coverage).

[232] Richelson & Evans *supra* note 3, at 13.

[233] *See Testing Intelligence*, THE ECONOMIST, Oct. 6, 2001, at 32..