Running head: WIRETAPPING: A NECESSITY

Wiretapping: A Necessity for Effectively Combating Terrorism in the 21st Century

Michael Hewitt

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2008

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial fulfillment of the requirements for graduation from the Honors Program of Liberty University.

_____

Thomas Metallo, Ph.D.
Chair of Thesis

_____

Faith Mullen, Ph.D.
Committee Member

_____

Stephen Witham, M.A.
Committee Member

_____

Marilyn Gadomski, Ph.D.
Assistant Honors Director

_____

Date

Abstract

In 2001, the Patriot Act was passed to provide new tools to combat terrorism. Chief among these new tools is the intelligence gathering method known as wiretapping. The role of wiretapping in the Patriot Act, particularly the constitutionality of this method, includes what criteria must be met to preserve constitutionally protected civil liberties. Wiretapping has had a significant effect as a facet of the Patriot Act on both the personal security and privacy of the American people. Current wiretapping policy lacks clear and appropriate guidelines addressing the modern terrorist threat. Future policy should reflect the need for new criteria to protect the national security and respect constitutionally imposed limits.

I. Wiretapping: A Necessity for Effectively Combating Terrorism in the 21st Century

1. *Four Main Categories of Wiretaps: Hardwired, Soft, Record and Transmit*

a. Hardwired wiretaps.

b. Soft wiretaps.

c. Record wiretaps and transmit wiretaps.

2. *The Patriot Act and Wiretapping*

II. Legal Basis for Wiretapping

1. *Federal Wiretap Act of 1968 (Title III) and the Electronic Communications Privacy Act*

2. *Foreign Intelligence Surveillance Act of 1978 (FISA)*

3. *Executive Order 12,333*

III. The Patriot Act's Effect on Existing Wiretap Laws

1. *Section 216*

2. *Section 203*

3. *Section 206*

4. *Section 217*

5. *Section 218*

IV. Constitutional Limitations on Wiretapping

1. *Separation of Powers*

2. *Fourth Amendment*

V. Effects of Wiretapping on Post 9-11 Society

Wiretapping: A Necessity for Effectively Combating Terrorism in the 21st Century

In the 21st Century, security is something that is increasingly hard to attain. Technology has revolutionized the way people communicate. This revolution has transformed the world into a global village, where a person may communicate instantly with any part of the globe. Living in this global village has its benefits, but it also has its consequences. Among these is an unprecedented vulnerability to attack of which this country has never before seen. The events of September 11, 2001 highlighted just how pregnable the United States now is. Terrorists are able to utilize these modern means of communication to disrupt and destroy life in America in a way that was not possible a few decades ago. In the tragic events of September 11, terrorists sponsored by the group al Qaeda were able to infiltrate the U.S., communicate and receive instructions with group leaders in the Middle East, and hijack airliners to crash into skyscrapers. In order to combat the growing threat posed by terrorism, new methods of combating those who seek to harm the U.S. have been undertaken. This has been accomplished primarily through legislation such as the Patriot Act, which has been crafted to develop new tools for counter-terrorism forces. One such tool that has caused tremendous controversy since 9-11 is the surveillance method known as wiretapping. Wiretapping is a constitutional and necessary tool for effectively combating terrorism and protecting the national security of the United Sates. This method will be analyzed, along with its role in the Patriot Act. Following this, the constitutionality of the wiretap method, with particular emphasis on what criteria must be met to preserve constitutionally protected civil liberties. Once this is accomplished, the effects which wiretapping has had on both the personal security and privacy of the American people. Finally, how current policy must

be changed to better protect national security while respecting the limits set forth in the Constitution.

Four Main Categories of Wiretaps: Hardwired, Soft, Record and Transmit

Hardwired wiretaps. Wiretapping is an intelligence gathering procedure, used to obtain high quality information without being detected. This activity "involves tying into a wire or other conductor", which is being used to transmit some form of message (Atkinson, 2005, para. 8). Most often the "wire is a telephone line, PBX (private branch exchange) cable, a local area network, CCTV video system, an alarm system, or any other communications medium" (Atkinson, 2005, para. 9). Wiretaps fall into four main categories depending on how they work. These categories are "hardwired, soft, record, and transmit" (Atkinson, 2005, para. 6).

The first of the four categories of wiretaps is the hardwired wiretap. A hardwired wiretap is "when physical access is gained directly to a section of wire" that the signal travels on (i.e. telephone line) (Atkinson, 2005, para. 10). A second wire is then attached to the main wire (normally through the use of an "isolation or slave device"); "the signal is then transmitted back to a secure location" (Atkinson, 2005, para. 10). This type of wiretap when discovered is fairly easy to trace back to the listening post (Atkinson 2005). An "isolation or slave device", is a device which is used to connect the telephone line being monitored to the wire being used to divert the communications signal back to the "listening post", where it is then monitored (Atkinson, 2005, para. 11; Communications 2007). It is difficult to trace this type of wiretap because, it "allows eavesdropping on the target telephone line to be performed from any telephone in the world" (Atkinson, 2005, para. 11; Communications, 2007, para. 30).

Soft wiretaps. Another form of wiretap is the soft wiretap. This wiretap is the preferred method for phone tapping, and consists of "a form of wiretapping implemented in the telephone company's equipment which … works by analyzing digital information as it passes through the telephone company's switching computer" (Telecommunications, 2008, para. 21). This modification can be done at the private branch exchange (PBX) of a business, or at the telephone company itself (Atkinson 2005). Soft wiretaps are "easy to catch on a PBX, but tougher to find in the phone company's system" (Atkinson, 2005, para. 15). This is because locating a soft wiretap "requires completely un-restricted access to the inner workings on the phone company's computers", which may be difficult to get (Atkinson, 2005, para. 15). This form of wiretap is often referred to as "REMOBS (REMote OBServation), DATU, ESS, or a translation tap (and) … are popular with large law enforcement agencies, intelligence agencies, larger corporations, and with hackers who find it quite simple to gain access via maintenance software" (Atkinson, 2005, para. 15).

Record wiretaps and transmit wiretaps. The last two categories of wiretaps are record wiretaps and transmit wiretaps. Record wiretaps are similar to hardwired wiretaps in that they are wired directly into the line transmitting the signal. This form of wiretap is simply "a tape recorder wired into a phone line" (Atkinson, 2005, para. 15). The tapes for record wiretaps must be changed regularly and therefore there is an increased risk of exposure for the person changing the tapes; for this reason record wiretaps are dangerous to use. Record wiretaps "are popular with amateur spies and private investigators" (Atkinson, 2005, para. 16). Another simple type of wiretap is the transmit wiretap. These phone taps consist of "a radio frequency (RF) transmitter connected to a signal

wire" (Atkinson, 2005, para. 16). This type of wiretap generates a large amount of energy, which increases the likelihood of its being detected by a knowledgeable bug sweep specialist. When wiretaps are properly installed, they are difficult to detect (Huitema 1999). Doing so requires a bug sweep expert who has a "high level of technical expertise and a large amount of equipment" (Atkinson, 2005, para. 16).

The Patriot Act and Wiretapping

The subject of wiretapping has come to national prominence as a facet of the controversial Patriot Act of 2001. The Patriot Act was enacted soon after the September 11, 2001 terrorist attack on the Pentagon and World Trade Center (Daniels 2006). The goal of the act is to "deter and punish terrorist acts in the United States and around the world, and to enhance the investigatory tools" used by law enforcement to do so (Electronic, 2001, para. 2). The word Patriot is an acronym for the bill's stated goal of "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (Herman, 2006, para. 1). Wiretapping composes a significant part of the Patriot Act. Sections 203, 206, 217, and 218 of the act help constitute this key method of gaining crucial intelligence, in an undetected manner, on national security threats (Doyle 2001; Podesta 2002). Section 203(b)(6) (Stat. 279) does this by stipulating that

> Any investigative or law enforcement officer … (who) has obtained knowledge of the contents of any wire, oral, or electronic communication … may disclose such contents to any other Federal law enforcement (officer) … to the extent that such contents include foreign intelligence or counterintelligence or foreign intelligence information (USA Patriot Act, p. 115).

Section 206 (Stat. 282) expands the government's authority to conduct a wiretap to

include "circumstances where the Court finds that the actions of the target of the application (wiretap) may have the effect of thwarting the identification of a specified person" (USA Patriot Act, p. 115). Section 217 (2)(i) (Stat. 291) prescribes that "It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser" (USA Patriot Act, p. 115). Finally, Section 218 (Stat. 291) helps to implement the wiretap method, by requiring that gathering "foreign intelligence information" be a "significant purpose" of government surveillance (USA Patriot Act, p. 115).

President George W. Bush, one of the main proponents of the use of wiretapping in the Patriot Act, considers wiretapping to be crucial in preventing terrorists from attacking America (ABCNews 2006). Bush has pointed out that wiretapping is "a vital part of the war on terror" (ABCNews, 2006, para. 5). In a speech on January 26, 2006 Bush explained that the war on terror "is a different kind of war with a different kind of enemy", and for this reason, new tools must be used if the U.S. is to win this war (ABCNews, 2006, para. 7). As evidence of this fact, Bush argues that

> two of the September 11 hijackers who flew the plane into the Pentagon -Khalid Almihdhar and Nawaf Alhazmi- communicated while they were in the United States to other members of al Qaeda who were overseas, but we didn't know they were here until it was too late (Arena, 2005, para. 6; Cooperative 2008; Porter 2003).

The NSA, FBI, and others were not aware of this fact until the terrorist attacks had already taken place. If the programs implemented in the Patriot Act had already existed, then these hijackers may have been located and identified in time to be stopped.

For this reason, wiretapping is a crucial part of the Patriot Act's goal of detecting and preventing possible terrorist attacks on the U.S. and abroad (Longley 2008).

Legal Basis for Wiretapping

Federal Wiretap Act of 1968 (Title III) and the Electronic Communications Privacy Act

Sections 203(b)(6), 206, 217 (2)(i), and 218 of the Patriot Act address the subject of electronic surveillance and specifically that of wiretapping (Doyle 2001; Podesta 2002). These sections however generally only serve to expand power which the government already has in this area. Much of the basic framework for the constitutional authority of the government to conduct wiretaps is grounded in previous legislation, specifically, The Federal Wiretap Act of 1968 and the Electronic Communications Privacy Act; The Foreign Intelligence Surveillance Act of 1978; and Executive Order 12,333 (Kennedy & Swire, 2003).

The first of these pieces of legislation is Title III of the Omnibus Crime and Control Act of 1968 (18 U.S.C. § 2510), and its subsequent revision in 1986, known as the Electronic Communications Privacy Act (18 USC § 2510; Kennedy & Swire, 2003). Title III, known Federal Wiretap Act, set many of the basic procedures for constitutionally conducting a wiretap. It was through this act that Congress "sought to enact a statutory wiretapping scheme that satisfied the Fourth Amendment requirements" which had been previously been established in the court case Berger v. New York (Monnat & Ethen, 2004, para. 24). In 1967 the *Berger* case had established a set of fundamental criteria governing the use of wiretaps (Monnat & Ethen 2004). In this case, the court "identified the… requirements for an interception (wiretap) order to be

constitutional under the Fourth Amendment" (Monnat & Ethen, 2004, para. 24). These are:

> (1) there must be probable cause to believe that a particular offense has been or is being committed; (2) the conversations to be intercepted must be particularly described; (3) the surveillance must be for a specific, limited period of time; (4) if the warrant is to be renewed, continuing probable cause must be shown; (5) surveillance must terminate once the conversation sought has been seized; (6) notice must be provided unless a factual showing of exigency is made; and (7) a return must be made on the warrant so the court may supervise and restrict the use of the seized conversations (Monnat & Ethen, 2004, para. 35; Berger v. New York).

The Federal Wiretap Act also stipulates that

> before a wiretap may commence, a warrant must be issued by a judge who must conclude, based on an affidavit submitted by the government, that there is probable cause to believe that a crime has been, is being, or is about to be committed (Center, 2005, para. 37).

These crimes included “terrorist bombings, hijackings, and other violent crimes, (however) … the Patriot Act expanded the list of criminal statutes for which wiretaps may be used” (Center, 2005, para. 38). If a wiretap is to be used before a crime has been carried out, it must be used for the purpose of identifying planning and conspiratorial activities. Since the passage of this act, judges have almost never denied the government a request for wiretap orders (Rahavy 2003). In 1986, passage of the Electronic Communications Privacy Act amended Title III (Catholic 2007). This amendment was added to extend government restrictions to include “interception of electronic

communications and access to stored electronic communications" (Catholic, 2007, para. 21; Belskis 2006).

Foreign Intelligence Surveillance Act of 1978 (FISA)

Sections 1801 and 1802 of the Foreign Intelligence Surveillance Act (FISA) of 1978 (US Code: Title 50, 1801-1802) established the criteria for wiretapping "aliens and citizens in the U.S." (Center, 2005, para. 21). Wiretaps used for this purpose must be "based on a finding of probable cause to believe that the target is a foreign power or an agent of a foreign power" (Elsea, 2003, para. 34; Stolz 2002; Hoffman 2003). For Americans and full-time resident aliens, there need also be "probable cause to believe that the person is engaged in activities that 'may' involve a criminal violation" (Center, 2005, para. 34). If an alien is not a full-time resident of the U.S. then "suspicion of illegal activity is not required- for them, membership in a terrorist group is enough, even if their activities on behalf of the group are legal" (US Code: Title 50 §1801(a)(1)(2)(3); Center, 2005, para. 16; McMillion 2006). The Patriot Act expanded FISA "to allow prosecutors to use wiretaps for the purpose of gathering evidence in criminal investigations of national security crimes" (Center, 2005, para. 40). Intelligence gathering activities taking place outside of the U.S. are not addressed in Title III or FISA (Kennedy & Swire 2003).

Executive Order 12,333

Legal power for activities occurring "outside of the U.S. is derived solely from Executive Order 12,333, issued by President Reagan in 1982, still in effect today" (Center, 2005, para. 41). Under Section 1, and Section 2.3 of this order, a warrant is not needed in order conduct surveillance on activities not occurring inside the U.S. If the person under surveillance is an American citizen or legal resident alien, then the Attorney

General must certify the surveillance (The Federal Register 1981; Kennedy & Swire 2003). "The Attorney General must find that there is probable cause to believe that the U.S. person who is the target of the surveillance is an agent of a foreign power as defined in FISA" (Center, 2005, para. 47). The decision to "target non-U.S. persons" is left entirely "up to the intelligence community", and no outside approval is required (Strickland, 2003, para.13). There are however, limitations on the promulgation of "information about U.S. persons that is collected incidentally to an intelligence collection activity" (Center, 2005, para. 35). Both FISA and Title III contain an exception for conducting wiretapping activities "in emergency situations that involve risk of death or serious bodily injury and in national security cases" (Center, 2005, para. 35). Wiretapping is allowed under these circumstances without judicial approval.

The use of roving taps is permitted under Title III and the authority to do so was "substantially broadened in 1999" (Center, 2005, para. 16). Section 206 of the Patriot Act added "roving tap authority to FISA" (Center, 2005, para. 16; Podesta 2002). Roving tap authority "allows the government to get a court order that does not name a specific telephone line or e-mail account but allows the government to tap any phone line, cell phone, or Internet account that" is used by the target (Privacy, 2008, para. 17). The use of roving taps is a somewhat rare occurrence. In 2005 for example, only eight roving taps were permitted under Title III for use in criminal cases (Duff 2006). The utilization of encoding in communication is not governed under U.S. law. If a communications company has encoded files, and subsequently is served with a wiretap order, it must then decrypt the communication. However, the "service provider has no obligation to decrypt communication (that has been) encrypted by the end user, when the service provider does

not have the key" (Center, 2005, para. 50). This has not been much of a problem for government surveillance activities. According to the 2006 Wiretap Report, no federal wiretaps encountered any encrypted communication. State and local wiretaps encountered thirteen encrypted communications, but "the encryption was not reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted" (Center, 2007, para. 51). Since 2000 "the government has only reported one wiretap" that has been impeded by encryption (Center, 2007, para. 52).

The Patriot Act's Effect on Existing Wiretap Laws

Section 216

The Patriot Act, enacted on October 26, 2001 "substantially changed the legal structure within which law enforcement and intelligence communities" may conduct electronic surveillance including wiretapping (Podesta, 2002, para. 14). The more substantive alterations to existing wiretap legislation are found in sections 203(b)(6), 206, 217 (2)(i), and 218 of the act. These changes updated and expanded existing surveillance powers to properly meet modern day challenges facing national security (Kennedy & Swire, 2003).

The first change was in the area of "law enforcement access to information about computer use (such as) Web surfing" (Podesta, 2002, para. 20). Section 216(a)(b) of the Patriot Act expands regulations to authorize the "installation of devices to record all computer routing, addressing, and signaling information. The government is able to access this information by certifying that the information likely to be obtained is relevant to an ongoing criminal investigation" (Podesta, 2002, para. 21). The ability to access personal computer information is a tremendous power because with it, the government is

able to learn vast amounts of information about a person. With such great power also comes a great potential for abuse, such as citizen profiling and invasion of privacy. Safeguards, such as strong judicial oversight, must be built into any broad expansion of governmental surveillance power. One safeguard that had always been in place to safeguard U.S. residents from illegal surveillance was the clear distinction that had been established dividing the foreign intelligence field from the domestic. Domestic intelligence gathering is subject to a much stricter set of guidelines than are foreign activities (Bedan 2007). The attacks of September 11, 2001 altered all of this. Several of the individuals involved in hijacking the planes used to crash into the World Trade Center had been in the country for some time. Better communication "between domestic law enforcement and foreign intelligence collection" may have been able to help stop these events from taking place (Podesta, 2002, para. 17). The Patriot Act facilitates this enhanced communication (Jones 2003).

Section 203

Section 203 of the act allows for "foreign intelligence information' gathered in criminal investigations by domestic law enforcement to be shared with the intelligence community" (Podesta, 2002, para. 25). Foreign intelligence agencies now have access to critical information that prior to 9-11 they may have not been able to access. The definition of "foreign intelligence information" provided in the Patriot Act is somewhat broad (Podesta, 2002, para. 25). "This information is defined as information relating to capabilities, intentions, or activities of foreign governments or elements thereof, and also foreign organizations, foreign persons or international terrorist activities" (Podesta, 2002, para. 30; Doyle 2001). Also included in the definition, is information regarding

Americans which relates to foreign powers or territories related to “the national defense or security of the U.S., or the conduct of its foreign affairs” (Podesta, 2002, para. 30). Because section 203 provides the “sharing of a broad range of information” about U.S. persons, it is necessary that this power be tempered with judicial restraints (Podesta, 2002, para. 30). The Patriot Act also modernized the authority the government has under FISA for "domestic intelligence gathering related to foreign powers" (Podesta, 2002, para. 30). Under FISA the government was required to get “a separate court order for each communication carrier used by a target” (Podesta, 2002, para. 31). Since modern technology allows a person to use a variety of communication devices -“cell phones, pay phones, e-mail, instant messaging, and wireless e-mail devices such as a BlackBerry”- in a matter of minutes, this requirement posed a significant barrier to monitoring the communications of an individual (Podesta, 2002, para. 40; Collins 2008).

Section 206

Section 206 of the Patriot Act changed this by allowing a “single wiretap to ‘roam’ from device to device, essentially tapping the person rather than the device” (Podesta, 2002, para. 31). Roaming wiretaps had been approved for use in criminal investigations as early as 1986. “Criminal investigations are generally subject to much stricter standards than are FISA intelligence-gathering activities, and so extending the authority to” the powers granted in FISA was a logical step (Podesta, 2002, para. 37; Doyle 2001). There is however, one significant difference between the criteria governing roaming wiretaps set forth in pre-existing criminal law and that set forth in the updated FISA requirements. This “is that criminal law requires law enforcement to ascertain that the target of a wiretap is actually using a device to be tapped” (Podesta, 2002, para. 33).

Section 206 of the Patriot Act does not include this type of provision. The lack of criteria governing when roaming wiretaps may be employed allows a much greater possibility for misuse, and a provision establishing such criteria is necessary (Cusick 2003).

Section 217

Section 217 of the statute "allows law enforcement, with permission of the owner, to monitor a computer trespasser's actions without obtaining an order for a wiretap" (Podesta, 2002, para. 47). This section applies the same authority to computer trespassers as is applied to trespassers unlawfully entering a home. As long as the owner of the home or computer grants permission, the police may enter without a warrant (Doyle 2001; Podesta 2002). This is a useful provision in that it limits the ability of hackers to utilize computers belonging to other owners. Section 217 also allows for a quick response "to malicious hacking, such as denial of service attacks" (Podesta, 2002, para. 47; Harper & Cinquegrana 2002).

Section 218

A final section of the Patriot Act that has changed the way electronic surveillance is conducted is section 218. Previously under FISA, a special court was created to oversee the surveillance of Americans. This court's purpose is to guarantee that any surveillance taking place in the continental U.S. is done with the sole "purpose of obtaining foreign intelligence information" (Electronic, 2001, para. 14). The creation of this court was an attempt "to balance the need to collect foreign intelligence information with the constraints of the Fourth Amendment", and also to help guarantee Americans protection of First Amendment rights (Podesta, 2002, para. 40; Doyle 2001). The difficulty has come when "foreign intelligence investigations uncover criminal

wrongdoing and lead to an investigation of the criminal conduct" (Podesta, 2002, para. 45). The use of the sole purpose test in these types of situations has created operational difficulties. The 9-11 terrorist attacks only served to break down the division between surveillance activities occurring outside the U.S., and those occurring in it. It has become increasingly important for intelligence and law enforcement communities to have the ability to jointly work a case and share information. (Hoffman, 2003) Section 218 alleviates some of this strain by only requiring that "foreign intelligence information be a significant purpose of (domestic intelligence) rather than the sole purpose" (Collins, 2002, para. 22).

Constitutional Limitations on Wiretapping

Separation of Powers

The provisions regarding wiretapping found in both Title III and FISA are all grounded in the limitations set by the Constitution. It is the Patriot Act's expansion of government power in these areas that presents a potential need to reevaluate the constitutionality of current wiretapping methods. Opponents of the controversial Patriot Act, such as Senator Bernie Sanders (I- VT), argue that the provisions must be revised because they are unconstitutional, and because they lead to an increased risk of civil liberty violations (Johnson 2003). Sanders warns that the increased powers given to the government by the Patriot Act make it "a bad and dangerous piece of legislation" (Johnson, 2003, para. 13). "The Patriot Act was passed in a blind rush, and in that rush to judgment, Congress trampled some important civil liberties" agrees fellow Representative Barbara Lee (D- CA), who describes the Patriot Act as a piece of legislation which ignores consequences (Johnson, 2003, para. 15). On the other side of

the issue are the proponents of the act, such as former Attorney General John Ashcroft, who point to the government's increased need for tools with which to combat terrorism and threats to national security, as the primary impetus for leaving the act unchanged (Johnson 2003). According to Ashcroft, "those who seek to limit the federal government's new anti-terrorism tools are hindering progress against those who would harm Americans" (Johnson, 2003, para. 16). Ashcroft, one of the most avid defenders of the Patriot Act, is quick to point out that

> Not a single court in America has validated any of the charges of violations of Constitutional rights in connection with the Patriot Act. On … every … tool provided in the Patriot Act, charges of abuse of power are ghosts, unsupported by fact or example (Johnson, 2003, para. 16).

The solution lies in sponsoring legislation that both actively protects national security and combats terrorism, while preserving the civil liberties of every American (Longley 2008). While increased authority to conduct wiretaps has been conceded by critics of the Patriot Act as necessary, the lack of judicial limits set in place to ensure that this authority remains constitutional has been the major cause of concern. At the heart of the constitutional controversy surrounding electronic surveillance lays two basic issues: separation of powers and the Fourth Amendment. Those opposed to sections pertaining to electronic surveillance in the Patriot Act, are concerned first that the President does not have the constitutional authority to order these types of surveillance programs, and secondly, that these "provisions violate the Fourth Amendment prohibition against illegal searches and seizures" (CRFC, 2005, para. 47; Longley 2008; Hoffman 2003).

The Patriot Act expands the legal authority of the Executive in deciding national

security matters. Section 217 in particular of the act, increases the authority of the FBI so that it "can acquire bank records and Internet or phone logs of a person … without first seeking approval from a judge" and without the "need to show probable cause" (Singel, 2003, para. 34). Other pieces of legislation, such as the Authorization for Use of Military Force in Response to the 9/11 Attacks (AUMF) and the Protect America Act of 2007 also greatly increase the power of the Executive, by permitting the Executive to order the use of force (including wiretaps) against national security threats, with little to no judicial oversight (Berger 2006). Proponents of the expanded statutory authority recently granted to the Executive in these areas, argue that it is authority which is already given to the Executive in the Constitution. These proponents offer several legal theories defending the constitutionality of such provisions, all of which are based on the fact that Executive authority is grounded "in Article II, Section 2 of the U.S. Constitution, which makes the President the Commander-in-Chief of the U.S. military" (Whitehouse, 2008, para. 8). Notable among these theories, is the Unitary Executive Theory, which argues that if Article II of the Constitution gives the President the "responsibility to protect" the United States then it obviously gives the President the power to protect the country (SourceWatch, 2008, para. 46; Longley 2008). One particular proponent of this theory, Supreme Court Justice Samuel Alito, has "advocated his personal legal view supporting the Unitary Executive Theory before…" (Democrats, 2006, para. 5). In describing this theory of Executive power, Alito argues that "The president has not just some Executive powers, but the Executive power -- the whole thing" (Democrats, 2006, para. 6). According to this theory, "all Executive authority must be in the President's hands, without exception" (SourceWatch, 2008, para. 46).

It is under this view of Executive authority that proponents of the act defend the constitutionality of the electronic surveillance provisions. This authority allows the president "to deploy military force preemptively against terrorist organizations or the states that harbor or support them, whether or not they can be linked to the specific terrorist incidents of September 11" and that wiretapping is such an activity that the President has the inherent authority to engage in (Center, 2005, para. 50). Article II of the Constitution authorizes the President to command all members of the branches of the military (Findlaw 2008). The NSA, which is not a traditional branch of the U.S. military, has been responsible for conducting these disputed wiretaps. The NSA, while not a branch of the U.S. military, does employ a substantial number of military personnel. "Selected NSA employees also attend the various war colleges of the U.S. and the NSA serves as a training resource for the Department of Defense" (Longley, 2008, para. 18). If wiretap operations are conducted by military personnel then, argue proponents of the Patriot Act, the President is well within his constitutional authority to conduct them. Executive authority to use the NSA to conduct wiretaps is grounded in AUMF and the Protect America Act of 2007. The question is not so much, is it within the Executive's authority to use agencies such as the NSA to conduct wiretaps, but rather, does the Executive have the authority to order wiretaps. This is evidenced in several court cases challenging the Executive's authority in this area. These cases include Hepting v. AT&T, and ACLU v. NSA. In both cases the Executive's authority to conduct wiretaps is challenged as either violating the Fourth Amendment, or violating the Constitution's separation of powers. The cases do not however, challenge the fact that the Executive may order Federal agencies such as the NSA to conduct wiretaps (EFF 2007). Further

support regarding the inherent constitutional authority of the Executive to use Federal agencies to conduct wiretaps is found in both the Unitary Executive Theory, as well as the DOJ's White Paper on NSA Legal Authorities, entitled " Legal Authorities Supporting the Activities of the National Security Agency Described By the President"; both of which extensively analyze this issue (SourceWatch, 2008, para. 10; DOJ 2006).

On the opposing side, critics such as Senator Sheldon Whitehouse, argue that this is an "astoundingly broad assertion of Executive authority, and a staggering disregard for basic principles of separation of powers, and the structure of our government" (Whitehouse, 2008, para. 17). These critics point out that allowing the Executive such far reaching powers, erodes the traditional checks and balances of governmental power, specifically by increasing "Executive authority at the expense of judicial second opinions about when searches and seizures are reasonable" (Herman, 2006, para. 24). This is the view expounded by Portland State University law professor Phillip Cooper, who agrees that "There is no question that the Bush administration has been involved in a very carefully thought-out, systematic process of expanding presidential power at the expense of the other branches of government" (Savage, 2006, para. 35). According to this point of view, the Patriot Act allows the Executive to have unchecked power with which to conduct surveillance activities such as wiretapping. While the President does have the duty to preserve, protect, and defend the Constitution, his power to do so does have limits. The claim that Patriot Act exempts the Executive branch from any political accountability is invalid, because without accountability, none of the constitutional structures can work (Podesta 2002; Ackerman 2006). The issue of Executive

infringement on constitutional checks balances and remains very controversial.

Fourth Amendment

The Patriot Act's broad delegation of Executive power has been the subject of much criticism, as have many of the national security measures contained in the bill. These counter-terrorism measures also have been deemed as violating civil liberties, particularly those granted in the Fourth Amendment of the Bill of Rights. The Fourth Amendment grants

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (Findlaw, 2008, para. 6).

Critics of the Patriot Act claim that it violates this "amendment by allowing the government" unrestricted power to search and seize information without demonstrating probable cause (Fisher, 2005, para. 5). This is the view expressed by Senator Russ Feingold, who warns that due to the Patriot Act, "The privacy of law-abiding Americans is at stake, along with their confidence in their government" (Fisher, 2005, para. 17). The Fourth Amendment requires law-enforcement officers to obtain warrants "before a judge describing particularly the place to be searched, and the persons or things to be seized" (Center, 2005, para. 22). The officers may only obtain a warrant if they can show the judge that there is "probable cause that the person is engaging in criminal activity" (Center, 2005, para. 15). After a warrant is obtained, "federal law demands that the officers still report to the court on the results of the search" (Center,

2005, para. 15). Wiretaps are included in the types of searches contingent upon warrants and the probable cause standard. The court in Berger v. New York confirmed these criteria, by dictating that in order to get a warrant, there must be "probable cause to believe that a crime has been, is being, or is about to be committed", and furthermore that the results garnered by a wiretap warrant must be reported back to the court (Monnat & Ethen, 2004, para. 30; Center 2005). There were however, certain exceptions to these Fourth Amendment requirements allowed under federal law, which existed before the passage of the Patriot Act in 2001. Among these were pen-trap exceptions, which involved acquiring telephone numbers dialed to and from a specific phone. "In order to get these numbers from the telephone company, officers must get a pen-trap order from a judge" (Constitutional, 2008, para. 10). This authority was granted to congress under 50 U.S.C. § 1842 (FISA). The officers do not however, need to show probable cause of criminal use, but must only "certify that the information is needed for an ongoing criminal investigation" (Constitutional, 2008, para. 10; The EFF 2002). The rationale for these relaxed criteria is that these records are less invasive than are other types of surveillance searches.

Another exception involved matters that went before the Federal Intelligence Surveillance Court. This court was formed in 1978 to regulate certain activities of U.S. intelligence agencies. The formation of this court was the result of a compromise among Congressional leaders, regarding the level of criteria these intelligence agencies would be required to meet in their surveillance activities. With the formation of the court, "Congress required U.S. intelligence agencies such as the FBI and NSA, to apply for warrants for wiretaps and other forms of surveillance on foreign governments and

agents. Because these agencies are not investigating domestic crime", they are exempted from the probable cause standard (CRFC, 2005, para. 9). The only criterion that they must meet is certifying that the purpose of the investigation they are seeking approval for "is to track a foreign government or agent" (CRFC, 2005, para. 9). The agencies are not required to "report to the court on the result of the surveillance" (CRFC, 2005, para. 10). "The effect of the Patriot Act was to expand these existing exceptions to the probable cause standard" (CRFC, 2005, para. 10). In section 215, the act allows the FBI to request a warrant from the Foreign Intelligence Surveillance Court "to search any tangible things related to the terrorism suspect" (Constitution, 2008, para. 4). The "any tangible thing" phrase found in section 215 "may include almost any kind of property -including books, documents, and computers" (CRFC, 2005, para. 10). Under section 215 authorizations, the "FBI may also monitor or seize personal records held by public libraries, bookstores, medical offices, Internet providers, churches, political groups, universities, and many other businesses and institutions" (CRFC, 2005, para. 11; "Our view" 2006). The FBI will be granted a warrant as long as it certifies that "the search is to protect against international terrorism or clandestine intelligence activities [spying]" (CRFC, 2005, para. 11; "Our view" 2006). Nowhere is the FBI required to meet the probable cause criteria. This newly formed criterion allows that a terrorism suspect may be "any U.S. citizen who the FBI speculates may be involved in terrorist activities" (CRFC, 2005, para. 11; "Our view" 2006). Under certain circumstances, these activities may even include First Amendment protected acts including non-violent public protests. In the event the FBI does seize information, the Patriot Act allows for third parties to be served with Section 215 orders. These orders prohibit third parties,

i.e. “Internet providers and public librarians, from informing anyone that the FBI conducted a search of their records” (CRFC, 2005, para. 11).

Section 216 “extends pen-trap orders to include e-mail and web browsing” (CRFC, 2005, para. 12). This section permits “the FBI to ask Internet service providers to turn over a log of the web sites that a person visits” as well as the "addresses of email that has been sent and received by the person’s computer" (CRFC, 2005, para. 12; Hoffman 2003). Another controversial provision of the act is section 213. This section permits the so-called sneak-and-peek searches, the constitutionality of which has been the subject of much controversy. This section authorizes these searches for all federal criminal investigations. The criteria that law enforcement officers must meet is to show that a "reasonable cause to believe (exists) that providing immediate notification… may have an adverse result on the investigation" (Ackerman, 2006, para. 10). If approved by a judge, the FBI is able to delay notification of the citizen about the search for a reasonable period of time. The rationale for allowing searches of citizens’ homes and business in secret is that "these searches may be needed to prevent destruction of evidence or the jeopardizing of an ongoing secret investigation" (Ackerman, 2006, para. 10).

Effects of Wiretapping on Post 9-11 Society

Effects on National Security

In analyzing post 9-11 wiretapping, it is necessary to analyze the effects that its use has had on national security and domestic society in the realm of National Security, wiretapping has proven to be instrumental in the identification and prosecution of

terrorists, effectively helping to diminish this threat. In the domestic realm, wiretapping has proven to be an effective means of preventing terrorist attacks in the U.S., and of putting Americans at ease.

The most obvious evidence that the use of wiretapping has been successful in protecting American national security is the "fact that there has been no serious terrorist incident on American shores since its passage in 2001" (Spangler, 2005, para. 13). Senator Orrin Hatch, R-Utah, and a staunch defender of the Patriot Act and its wiretapping provisions, has pointed out that “because of necessary secrecy laws, we may never know the full positive effects the Patriot Act is having on terrorism” (Spangler, 2005, para. 13). Hatch did however note that the Justice Department has credited key provisions of the Patriot Act with playing a role in the terrorism-related convictions of hundreds of suspects. It has largely been the tools of wiretapping and other forms of electronic surveillance, which have received the credit for the success of hundreds of anti-terrorism operations since 2001. Most notable among these operations was the "recent apprehension in England of scores of suspects, who were charged with making plans to blow up as many as ten airliners traveling to the United States" (Criminal, 2006, para. 24). In this operation, electronic surveillance played an instrumental part in allowing British agents to monitor the activities of a terrorist cell. "'We have been looking at meetings, movement, travel, spending and the aspirations of a large group of people' said Peter Clarke, head of Scotland Yard's anti-terrorism branch" (ABCNews, 2006, para. 2). In this case, British agents substantially monitored the terrorist cell before making the arrests. (ABCNews, 2006, para. 24) Another such situation was the uncovering of "evidence indicating that a Pakistani charity was diverting funds originally

contributed for earthquake relief to finance the planned terrorism attacks on these jumbo jets" (Criminal, 2006, para. 16). It is, however, difficult to attain the exact details of the results of these operations, because in these investigations, "details leading up to the filing of formal charges is not usually revealed" (Criminal, 2006, para. 16). It is known however, that since September 11, 2001 thousands of individuals classified as terrorists have been subjected to electronic surveillance procedures. The surveillance, specifically wiretapping, of individuals suspected of terrorist activities, has resulted in nearly a 20% conviction rate (Criminal 2006).

Effects on Domestic Society

The effect that the Patriot Act, specifically its wiretapping provisions, has had on domestic society, are also worth noting. Despite the heavy amount of criticism that has befallen these provisions, a variety of polls have shown that in the years following 9-11, Americans have cumulatively grown much more at ease in regard to their own personal security. In a nationwide poll taken by the *New York Times* and CBS News in September of 2006, only 22% of Americans "said that they were still very concerned about an attack occurring where they live" (Toner & Connelly, 2006, para. 4). This number is down from almost 40% five years ago. Seventy-five percent of Americans said that their daily lives had largely returned to normal (Toner & Connelly 2006). In the midst of this general feeling of security however, more than half of those surveyed "said they thought a terrorist attack on the United States in the next few months was “very” or “somewhat” likely" (Toner & Connelly, 2006, para. 4). While this number has decreased significantly since 2001, it still shows that a wary sense of caution is the outlook of a majority of Americans. With the rather substantial opposition the Bush administration has received

to its introduction of the Patriot Act and its subsequent revision in 2006, nearly 60% of those surveyed said they believe that the government has not done all that "could reasonably be expected" of it (Toner & Connelly, 2006, para. 6). Despite this find, there is a strong section of people in society who demand that some of the more invasive provisions of the bill be removed from the legislation.

This comes even after the subsequent revision of the act in March of 2006. This revision, known as the USA Patriot Improvement and Reauthorization Act, "adds additional judicial oversight to the original law" (Stolberg, 2006, para. 1). It gives "recipients of subpoenas the right to challenge an accompanying judicial order not to discuss the case publicly, though they do have to wait one year while complying with the subpoena in the meantime" (Swing, 2007, para. 7). The revision also prevents the FBI from "demanding the names of lawyers consulted by people who receive secret government requests for information, and would prevent most libraries from being subject to requests" for records (Swing, 2007, para. 7). Law enforcement officials still retain the power to "gather information about terrorism suspects who use libraries to access the internet", if they get the information directly from the internet service provider (Stolberg, 2006, para. 4).

Even though these civil liberties protections have been inserted in the revision, privacy infringements are still a major issue. Many are concerned that even the Reauthorization Act still does not accurately respect civil liberties. Senate Judiciary Committee Chairman Arlen Spector was concerned enough that he began drafting new legislation immediately after the passage of the Reauthorization Act, which he said "better comports with my own sensitivity to civil rights" (Spangler, 2005, para. 5).

Senator John Sununu joined in criticizing the revised Patriot Act by saying "Those that would give up essential liberties in pursuit (of) ... a little temporary security deserve neither liberty nor security," (Associated, 2005, para. 7). Critics such as Senators Spector and Sununu, contend that too many provisions of the revised act still remain the same, including not enough changes to those controversial provisions that did survive the revision process. These include the authority to intercept wire, spoken, or electronic communications, as well as the interception of wire or electronic communications of a computer hacker or intruder in certain circumstances.

Analysis of Future Wiretapping Policy

Wiretapping is a very useful tool for law enforcement. This intelligence gathering method provides a legal means of combating terrorism. The controversy surrounding the use of wiretapping centers around two things. These are the separation of powers and the Fourth Amendment. Future wiretapping policy should be developed in a form that preserves traditional checks and balances on government power thereby protecting civil rights, but that at the same time allows the government much needed flexibility in dealing with the mobile, ever-changing threat that is modern terrorism.

In order to create this kind of legislation, the foundational criteria governing the use of wiretaps, which has been laid down by previous laws and court decisions, must be analyzed and carried over into any new law impacting this area. These include specifically, the fundamental criteria laid down in Berger v. New York, and later given statutory authority in the Federal Wiretap Act of 1968 (Monnat & Ethen 2004). These criteria include "determining that there is a probable cause to believe that a particular offense has been or is being committed, the particular description of conversations to be

intercepted, a specific, limited time period, and the termination of the (wiretap) upon completion of the task" (Monnat & Ethen, 2004, para. 17). These fundamental criteria governing the use of wiretaps should form the basis of any future wiretapping legislation. Another significant principle that must be included in future legislation comes from the Supreme Court case Katz v. U.S. In this case, the Supreme Court dictated that a wiretap conducted without "antecedent justification", or prior approval by a court, violates the Fourth Amendment (Katz v. U.S., p. 6). *Katz* therefore establishes the important principle that in order to constitutionally conduct a wiretap, prior approval from a court must be received. It is interesting to note in the *Katz* decision that Justices Douglas and Brennan, agreed with the majority opinion with the exception of one notable point. Douglas and Brennan found that the one time when "no antecedent judicial authorization is necessary for electronic surveillance … is if the President of the United States or the Attorney General has authorized electronic surveillance as required by national security" (Katz v. U.S., p. 6).

In 1968 Congress passed the Federal Wiretap Act, which "sought to enact a statutory wiretapping scheme that satisfied the Fourth Amendment requirements announced in *Berger*" (Monnat & Ethen, 2004, para. 17). The Federal Wiretap Act forms the basis of all wiretapping legislation (Center 2005). In agreement with *Katz*, this act requires that "before a wiretap may commence, a warrant must be issued by a judge who must conclude, based on an affidavit submitted by the government, that there is probable cause to believe that a crime has been, is being, or is about to be committed" (Center, 2005, para. 40). Therefore, the basic principles founded in *Berger*, *Katz* and the Wiretap Act should be an important facet of any future wiretapping law. These do not however,

encompass all criteria to be considered. In 1972, the Supreme Court confirmed another important principle governing wiretapping, in the case U.S. v. U.S. District Court. The court's decision confirmed the principle that "prior judicial approval" is mandatory "before initiation of a search or surveillance …" (U.S. v. U.S. District Court, p. 10). What is particularly noteworthy in this case however is that the court found that prior judicial approval is required even in cases of a domestic security threat. In deciding this, they rejected the government's argument that in order "to protect the national security" the President may authorize surveillance "without prior judicial approval" (U.S. v. U.S. District Court, p. 10). The 1974 Supreme Court decision in United States v. Kahn helped to shed more light on the issue of how a warrant may be granted for a wiretap. In this decision the court confirmed three important criteria governing the use of wiretaps. These are (1) that a wiretap order may be given to include persons "as yet unknown" to be involved with the target of the order, (2) that the person named in the wiretap order does not need to be "a party to intercepted (communications)", and (3) that charges "may be brought against persons not formerly under investigation, due to evidence collected from a wiretap, and that the government does not have to prove that such persons would not have been implicated without the use of a wiretap" (United States v. Kahn, p. 11). The curbing of Executive authority to authorize wiretaps without judicial first permission, was ended somewhat with the terrorist attacks of September 11, 2001. It was in answer to these malicious acts that Congress passed the "Authorization for Use of Military Force in Response to the 9/11 Attacks (AUMF)" (Grimmett, 2007, para. 12). This piece of legislation is significant because Section 2(a) of the law

> authorizes the President 'to use all necessary and appropriate force against those

> nations, organizations, or persons he determined planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons' … The joint resolution further states, in Section 2(b)(1), Congressional intent that it 'constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution (Grimmett 2007).

President Bush describes this piece of legislation as "recognizing the authority of the President under the Constitution to take action to deter and prevent acts of terrorism against the United States" (Grimmett, 2007, para. 12). Bush takes this authority to include Executive authorization of warrantless wiretaps to protect national security. (Grimmett 2007) Executive wiretap authority has also recently been enhanced by passage of the Protect America Act of 2007, which legalizes warrantless wiretapping of foreign targets overseas (Bush 2007).

Future wiretapping legislation must be a balance between pre- and post 9-11 wiretapping criteria. Legislation must ensure that the Fourth Amendment will not be violated. This will be accomplished by ensuring that all future legislation contains the Fourth Amendment safeguarding criteria found in previous legislation. Future wiretap legislation must also ensure however that law enforcement agencies are able to combat national security threats in a timely manner. President Bush underscored this when he said, "To save American lives we must be able to act fast and to detect these conversations so we can prevent new attacks" (CNN, 2005, para. 15). One specific criterion which may be helpful in order to allow law enforcement to quickly respond to

terrorist threats is the ability to order a wiretap on a suspect, immediately, and without a warrant. President Bush does have the Executive authority to order wiretaps of this sort, under certain circumstances. This confirmed upon examination of Article II, Section 2 of the U.S. Constitution, which endows the Executive with the responsibility and power of being Commander-in-Chief of the armed forces, as well as through legislation such as AUMF, and the Protect America Act of 2007 (Findlaw 2008). What President Bush does not have is the authority to order warrantless wiretaps without being subject to any guidelines. This type of unlimited Executive power is granted nowhere in the Constitution. For this reason, future legislation should include something similar to the warrantless wiretapping criteria specified in the AUMF bill. This would provide law enforcement the ability to conduct wiretaps quickly and effectively, while still being subject to traditional Fourth Amendment criteria. These criteria would then be able to be adjusted in order to evolve along with the changing needs of national security. In this way a warrantless wiretap would not be very different from a regular judicially approved wiretap. It would still operate under the "probable cause" (Federal Wiretap Act 1968; 18 U.S.C. § 2510) standard. The warrantless wiretap would still be subject to a "specific, limited period of time" at the end of which it would be analyzed by all of the criteria used to analyze regular wiretaps (Berger v. New York, p. 6). By blending pre- and post 9-11 wiretapping criteria, and by allowing the Executive the freedom to exercise his authority to protect the nation, while not disturbing constitutionally imposed checks and balances (i.e. judicial oversight), future wiretapping legislation could help to serve the needs of this great country better than ever before.

Future wiretapping policy must be also be made to correct the flaws the have been perceived in existing policy. Legislation must ensure that civil liberties are safeguarded as much as is possible. This means "placing new limitations on the government's use of secret search and surveillance powers" (Stolberg, 2006, para. 7). This can be accomplished by tightening restrictions on the use of wiretaps. Wiretapping policy must be changed in regard to the distinction between domestic and foreign surveillance. More stringent criteria must be added to existing legislation clearly differentiating between the two types. The NSA is currently barred from domestic surveillance unless it gets special permission from the FISA court. Part of the controversy regarding domestic versus foreign surveillance is that there is often no clear criteria for determining exactly which category the object of the surveillance falls into. If a U.S. citizen is involved with international groups, or suspected of any threatening foreign communication, then he is easily lumped into the foreign surveillance category, and most wiretapping regulations no longer apply. Any U.S. citizen should be protected from unregulated surveillance unless it has been proven that there is probable cause to believe that he poses a threat to America. With a strict criteria clearly differentiating between domestic and foreign surveillance, foreign surveillance activities will be able to flow more freely, because national security agencies are already allowed almost unregulated surveillance of all non-U.S. persons.

One facet of wiretapping policy that must not be changed in the future is the ability of the government to authorize roving wiretaps. Roving wiretaps effectively wiretap a person, rather than a sole communication device. This disallows subjects of surveillance from simply switching from communication device to communication

device to avoid being tapped by law enforcement. This form of wiretap has been controversial because it allows the government to tap into a person's phone and listen to and record calls indiscriminately, and without any prior judicial approval. Under current wiretap law, if the government suspects that your telephone is being used for illegal activities, they may tap your phone. While roving wiretaps must be available to law enforcement agencies to fight terrorism, stricter criteria governing the use of such wiretaps, as well as the inclusion of judicial oversight, should be considered for future wiretapping policies. A judicial review of extended roving wiretaps, as well as a periodic random review of selected roving wiretap activities, would also help to keep the program accountable to the American people, and ensure that the government does not overstep its bounds into the privacy of American's lives.

Provisions must also be added to future legislation granting immunity to non-governmental groups which have been included in the terrorism surveillance process. This has been accomplished to some extent by the Protect America Act. These groups include telephone companies and Internet service providers, both of which have faced many lawsuits in return for their cooperation with government anti-terrorism activities. Private companies assisting the government in protecting national security should not be penalized for their cooperation. If their activities are found to be unconstitutional or illegal, and their actions have been committed solely to cooperate with government requests, then the government should be held responsible.

Along with increased judicial oversight, future wiretapping policy must also continue to implement the probable cause standard. To receive a warrant, law enforcement officers should be required to show that they have "probable cause to

believe that a crime has been, is being, or is about to be committed" (Berger v. New York, p. 8). The exceptions found in both FISA and Title III, pertaining to the conduction of wiretapping activities in situations that are of an emergency nature and in national security cases, should be continued. In these extreme circumstances wiretapping should be allowed without prior judicial permission. For the targeting of U.S. citizens with suspected terrorist links, the permission of the Attorney General should be required. This is already a part of current legislation and should also be contained in future revisions. Wiretapping is a constitutionally allowed form of surveillance. The President is well within his Article II authority in enacting legislation permitting it. The Constitution allows the President as Commander-in-Chief to use preemptive measures against enemies of the United States-both abroad and at home. Wiretapping is a preemptive measure. It is a necessary form of covert intelligence gathering that helps to keep the nation safe. The clearest evidence of its effectiveness is the fact that no serious terrorist act has occurred on U.S. soil, since the enactment of the wiretapping provisions of the Patriot Act in the days after September 11. There is much that must be done to ensure that the civil liberties of Americans are not infringed upon by this form of surveillance. Limitations upon Federal power should be applied as long as it is done in a manner that still allows law enforcement agencies to do their job of protecting the nation's security. Provisions such as wiretapping will help to keep this country a safe place, well into the 21st century. Wiretapping is a necessary, yet controversial tool in the war on terror. It is imperative that any future revisions to the law contain criteria for incorporating more judicial oversight into surveillance legislation. A balance must be struck in allowing law enforcement agencies enough freedom to do their job effectively,

while at the same time ensuring that safeguards are in place that protect people's civil liberties. Law enforcement agencies must be kept accountable with the power that is given them in the war on terror, however they must continue to be allowed the necessary tools and authority to continue to act immediately and effectively in tracking suspects. The need to achieve a balance between preserving American civil rights and properly securing Americans from attack is a difficult yet necessary goal to attain, and it is the future of the citizens of this great country to do so.

References

18 USC § 2510. (1986). "Electronic Communications Privacy Act."

18 USC § 2510. (1968). "Federal Wiretap Act."

ABCNews.com. (2006, August 10). Inside the U.K. Terror Plot. Retrieved March 9, 2008, from http://blogs.abcnews.com/theblotter/2006/08/inside_the_uk_t.html

ABCNews.com. (2006, January 23). Bush Calls Wiretapping a Vital Part of War on Terror. Retrieved March 21, 2008, from http://i.abcnews.com/US/story?id=1532436

Ackerman, B. (2006). Terrorism and the constitutional order. *Fordham Law Review*, *75.2*(November), 475-488. Retrieved March 3, 2008, from http://find.galegroup.com.ezproxy.liberty.edu:2048/itx/start.do?prodId=LT LegalTrac.

Arena, Kelli. (2005, December 17). Bush says he signed NSA wiretap order. *CNN.com.* Retrieved March 22, 2008, from http://www.cnn.com/2005/POLITICS/12/17/bush.nsa/index.html

Associated Press. (2005, December 15). Senate rejects reauthorization of Patriot Act. *MSNBC.com.* Retrieved February 24, 2008, from http://www.msnbc.msn.com/id/10485860/

Atkinson, J. M. (2005) Types of Wiretaps, Bugs and Methods. *Granite Island Group: Technical Surveillance Counter Measures.* Retrieved January 13, 2008, from http://www.tscm.com/typebug.html

Bedan, M. (2007, March). Echelon's effect: the obsolescence of the U.S. foreign intelligence legal regime. *Federal Communications Law Journal*, 425. Retrieved

January 13, 2008, from http://find.galegroup.com/itx/start.do?prodId=LT LegalTrac.

Berger, S. (2006, February 22). Crib Sheet: Wiretapping Without a Warrant. *CampusProgress.org.* Retrieved March 11, 2008, from http://www.campusprogress.org/tools/767/crib-sheet-wiretapping-without-a-warrant

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

Belskis, J. (2006, April 14). Applying the Wiretap Act to Online Communications after United States v. Councilman. *Shidler Journal of Law, Commerce + Technology*, *2*(1547-0695), 18. Retrieved March 21, 2008, from http://www.lctjournal.washington.edu/Vol2/a018Belskis.html

Bush, G. W. (2007, August 5). Fact Sheet: The Protect America Act of 2007. *The White House.* Retrieved February 5, 2008, from http://www.whitehouse.gov/news/releases/2007/08/20070806-5.html

Catholic University of America. (2007, November 16). Summary of Federal Laws. Retrieved March 26, 2008, from http://counsel.cua.edu/fedlaw/Ecpa.cfm

Center for Democracy and Technology. (2007, September 21). Statement of James X. Dempsey. Retrieved March 15, 2008, from http://www.cdt.org/testimony/20040908dempsey.shtml

Center for Democracy and Technology. (2005, October 11). The Nature and Scope of Governmental Electronic Surveillance Activity. Retrieved January 6, 2008, from http://www.cdt.org/wiretap/wiretap_overview.html

CNN.com. (2005, December 20). Bush: Secret wiretaps won't stop. Retrieved March 16,

2008, from http://www.cnn.com/2005/POLITICS/12/19/bush/index.html

Collins, J. M. (2002). And the Walls Came Tumbling Down: Sharing Grand Jury Information with the Intelligence Community under the USA PATRIOT Act. *American Criminal Law Review*, *Summer*(39 Am. Crim. L. Rev. 1261). Retrieved February 14, 2008, from http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?risb=21_T3331285835&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T3331285838&cisb=22_T3331285837&treeMax=true&treeWidth=0&csi=168966&docNo=1 LexisNexis Academic.

Communication Security Inc. (2007). Telephone Line Attacks. Retrieved March 19, 2008, from http://www.bugsweep.com/index.html

Constitutional Rights Foundation. (2008). The Patriot Act: What Is the Proper Balance Between. Retrieved March 9, 2008, from http://www.crf-usa.org/bria/bria19_4a.htm

Cooperative Research History Commons. (2008). Complete 911 Timeline: Monitored Al-Qaeda Hub in Yemen. Retrieved March 19, 2008, from http://www.cooperativeresearch.org/timeline.jsp?projects_and_programs=complete_911_timeline_yemen_hub&timeline=complete_911_timeline

CRFC. (2005). The Role of the Citizen in the 21st Century. Retrieved March 23, 2008, from http://www.crfc.org/pdf/2005summit.pdf

Criminal Terrorism Enforcement in the United States During the Five Years Since the 9/11/01 Attacks. (2006, December). *TRAC REPORTS*, 169. Retrieved January 30, 2008, from http://trac.syr.edu/tracreports/terrorism/169/

Cusick, K. R. (2003). Thwarting Ideological Terrorism: Are We Brave Enough to Maintain Civil Liberties in the Face of Terrorist Induced Trauma? *Case Western Reserve Journal of International Law*, *Winter*(35 Case W. Res. J. Int'l L. 55). Retrieved January 8, 2008, from http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?risb=21_T3331295078&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T3331295081&cisb=22_T3331295080&treeMax=true&treeWidth=0&csi=148375&docNo=1 LexisNexis Academic.

Daniels, M. S. (2008, December 12). A Phoenix from the Ashes of 9/11. *Silver State News Service.* Retrieved March 16, 2008, from http://www.silverstatenews.com/newssections/Entertainment/ashtuesday/index.html

Democrats.senate.gov. (2006, January 11). FACT CHECK: JUDGE ALITO ON THE THEORY OF THE UNITARY EXECUTIVE. Retrieved March 11, 2008, from http://democrats.senate.gov/judiciarycommitteesupremecourt/correcting-12.cfm

DOJ. (2006, January 19). Legal Authorities Supporting the Activities of the National Security Agency Described By the President 2006. 1-42.

Doyle, C. (2001, December 10). "Terrorism: Section by Section Analysis of the USA Patriot Act." CRS Report for Congress. 01431. The Library of Congress: Congressional Research Service. Retrieved March 21, 2008, from http://nsarchive.chadwyck.com/nsa/documents/TE/01431/all.pdf Digital National Security Archive.

Duff, J. C. (2006, May 13). 2006 Wiretap Report Administrative Office of the United

States Courts. Retrieved January 25, 2008, from www.uscourts.gov/wiretap06/contents.html

Electronic Frontier Foundation. (2007). NSA Multi-District Litigation: Documents Relating to All Cases and Dismissed Cases. Retrieved March 25, 2008, from www.eff.org/cases/att

Electronic Privacy Information Center. (2001, October 24). USA PATRIOT Act (H.R. 3162) Retrieved March 21, 2008, from http://epic.org/privacy/terrorism/hr3162.html

Elsea, J. (2003, May 19). Proposed Change to the Foreign Intelligence. *CRS Report for Congress*, (RS21472), 1-6. Retrieved March 24, 2008, from http://www.fas.org/irp/crs/RS21472.pdf

Federal Wiretap Act. (1968). 18 U.S.C. § 2510. Retrieved March 1, 2008, LexisNexis.

Findlaw.com. (2008). U.S. Constitution: Article II. Retrieved March 22, 2008, from http://caselaw.lp.findlaw.com/data/constitution/article02/

Findlaw.com. (2008). U.S. Constitution: "Fourth Amendment". Retrieved February 5, 2008, from http://caselaw.lp.findlaw.com/data/constitution/amendment04/ FindLaw.

Fisher, W. (2005, February 25). Senator Seeks to Curb Controversial "Patriot Act" *CommonDreams.org*. Retrieved March 2, 2008, from http://www.commondreams.org/headlines05/0225-10.htm

Foreign Intelligence Surveillance Act. (1978). 50 U.S.C.§§1801–1811,1821–29,1841.46a

Grimmett, R. F. (2007, January 16). Authorization for Use of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History. *CRS Report for Congress*, (RS22357), 6. Retrieved March 5, 2008, from http://64.233.167.104/search?q=cache:OEMWypte23IJ:www.fas.org/sgp/crs/natsec/RS22357.pdf+authorization+for+use+of+military+force+in+response+to+the+9/11+attacks&hl=en&ct=clnk&cd=1&gl=us

Harper, R. M. & Cinquegrana, R. J. (2002). THE USA PATRIOT ACT: AFFECTS ON AMERICAN EMPLOYERS AND BUSINESSES. *Boston Bar Journal*, *May/June*(46 B.B.J. 10). Retrieved March 12, 2008, from http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?risb=21_T3331308969&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T3331308972&cisb=22_T3331308971&treeMax=true&treeWidth=0&csi=156158&docNo=1 LexisNexis Academic.

Herman, S. (2006, January). PATRIOT Games: Terrorism Law and Executive Power. *JURIST Legal News & Research*. Retrieved January 3, 2008, from http://jurist.law.pitt.edu/forumy/2006/01/patriot-games-terrorism-law-and.php

Hoffman, G. A. (2003). Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment. *American Criminal Law Review*, *Fall*(40 Am. Crim. L. Rev. 1655). Retrieved January 27, 2008, from http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?risb=21_T3331320945&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T3331320948&cisb=22_T3331320947&treeMax=true&treeWidth=0&csi=168966&docNo=1 LexisNexis Academic.

Huitema, C. (1999, October 15). "IETF Wiretapping List (E-mail)" *The Internet Engineering Task Force.* Retrieved March 1, 2008, from http://www.ietf.org/

Johnson, J. (2003, September 25). Congressional Opponents Lash out at PATRIOT Act, Ashcroft. *CNSNEWS.COM.* Retrieved March 21, 2008, from http://www.cnsnews.com/ViewNation.asp?Page=%5CNation%5Carchive%5C200309%5CNAT20030925a.html

Jones, K. (2003). Comment and Casenote: The effect of the Homeland Security Act On Online Privacy and the Freedom of Information Act. *University of Cincinnati Law Review*, *Winter*(72 U. Cin. L. Rev. 787). Retrieved February 17, 2008, from http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?risb=21_T3331269642&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T3331269645&cisb=22_T3331269644&treeMax=true&treeWidth=0&csi=7376&docNo=1 LexisNexis Academic.

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

Kennedy, C. H. & Swire, P. P. (2003, June 30). State Wiretaps and Electronic Surveillance After September 11. *Hastings Law Journal*, (April 2003). Retrieved December 31, 2007, from http://www.constitutionproject.org/pdf/report_state_wiretaps_after_9_11.pdf

Longley, R. (2008). How Bush Will Defend His Wiretaps. *About.com: US Government Info.* Retrieved January 2, 2008, from http://usgovinfo.about.com/od/thepresidentandcabinet/a/bushdefense.htm

McMillion, R. (2006, August). BALANCING ACT. *ABA Journal*, *92*(8), 67. Retrieved February 1, 2008, from

http://web.ebscohost.com/ehost/detail?vid=4&hid=117&sid=c82d4c6c-15ff-46e1-8357-ef394283c571%40sessionmgr107 Academic Search Premier.

Monnat, D. E. & Ethen, A. L. (2004, March). A Primer on the Federal Wiretap Act and Its Fourth Amendment Framework. *Journal of the Kansas Trial Lawyers Association*, 12-15. Retrieved March 24, 2008, from http://www.monnat.com/Publications/Wiretap.pdf

Our View: Patriot Act better, but still not what we deserve. (2006, March 10). *Midland Daily News*. Retrieved January 22, 2008, from http://www.ourmidland.com/site/news.cfm?newsid=16280859&BRD=2289&PAG=461&dept_id=472539&rfi=6

Podesta, J. (2002). USA Patriot Act: The Good, the Bad, and the Sunset. *American Bar Association*, Winter. Retrieved February 1, 2008, from http://www.abanet.org/irr/hr/winter02/podesta.html

Porter, J. (2003). Osama Bin-Laden, Jihad, and the Sources of International Terrorism. *Indiana International and Comparative Law Review*, *13*, 871-885.

Privacy Alerts. (2008, April 21). Can people eavesdrop on my landline phone conversations? Retrieved March 23, 2008, from http://www.privacyalerts.org/eavesdropping.html

Rahavy, S. K. (2003). The Federal Wiretap Act: the Permissible Scope of. *JOURNAL OF HIGH TECHNOLOGY LAW*, *2*(1), 87-100. Retrieved January 14, 2008, from http://www.law.suffolk.edu/highlights/stuorgs/jhtl/publications/V2N1/SRAHAVYV2N1N.pdf

Rasch, M. (2006, January 12). Wiretapping, FISA, and the NSA. *The Register*. Retrieved

December 14, 2007, from http://www.theregister.co.uk/2006/01/12/us_wiretapping_laws/page5.html

Savage, C. (2006, April 30). Bush challenges hundreds of laws. *Boston.com.* Retrieved March 21, 2008, from http://www.boston.com/news/nation/articles/2006/04/30/bush_challenges_hundreds_of_laws/

Singel, R. (2003, November 24). Congress Expands FBI Spying Power. *Wired.* Retrieved March 13, 2008, from http://www.wired.com/politics/law/news/2003/11/61341

SourceWatch.org. (2008). Unitary Executive Theory. Retrieved March 17, 2008, from http://www.sourcewatch.org/index.php?title=Unitary_Executive_Theory

Spangler, J. (2005, July 17). Cannon, Hatch clash on 'sunset' for Patriot Act. *Deseret Morning News*. Retrieved January 22, 2008, from http://deseretnews.com/dn/view/0,1249,600149304,00.html

Stolberg, G. (2006, March 3). U.S. Senate approves revised Patriot Act. *Herald Tribune.* Retrieved March 10, 2008, from http://www.iht.com/articles/2006/03/03/news/patriot.php

Stolz, B. A. (2002, September). The Foreign Intelligence Surveillance Act of 1978: The Role of Symbolic Politics. *Law & Policy*, *24*(3), 269-298. Retrieved February 12, 2008, from http://web.ebscohost.com/ehost/detail?vid=4&hid=117&sid=c82d4c6c-15ff-46e1-8357-ef394283c571%40sessionmgr107 Academic Search Premier.

Strickland, L. S. (2003, February). Information and the War Against Terrorism, Part III. *American Society for Information Science and Technology*, *28*(3). Retrieved

March 26, 2008, from http://www.asis.org/Bulletin/Mar-02/strickland2.html

Swing the Vote. (2007, March 4). 10 Reasons to vote AGAINST Congressman Charlie Bass. Retrieved March 21, 2008, from http://swingthevote.us/download/reasons.doc

Telecommunications Surveilance. (2008). Telephone Transmitters. Retrieved March 20, 2008, from http://seussbeta.tripod.com/Tap.html#soft

The Electronic Frontier Foundation. (2002, August 2). EFF Analysis of the Cyber Security Enhancement Act. Retrieved January 2, 2008, from http://w2.eff.org/Privacy/Surveillance/?f=20020802_eff_csea_analysis.html

The Federal Register. (1981, December 4). The provisions of Executive Order 12333 46 FR 59941. The National Archives. 200. Retrieved March 1, 2008, from http://www.archives.gov/federal-register/codification/executive-order/12333.html

Toner, R. & Connelly, M. (2006, September 7). 9/11 Polls Find Lingering Fears in New York. *New York Times*. Retrieved January 5, 2008, from http://www.nytimes.com/2006/09/07/us/07poll.html?pagewanted=2&_r=1

US Code: Title 50, § § 1801-1802. (1978). "Foreign Intelligence Surveillance Act."

USA Patriot Act. (2001, October 26). Public Law Pub.L. 107-56.

United States v. Kahn. (1974). 415 US 143.

U.S. v. U.S. District Court. (1972). 407 U.S. 297.

Whitehouse, S. (2008). Executive overreaching in surveillance of Americans. *New Jersey Law Journal*, (January 7, 2008). from LegalTrac.