

RUNNING HEAD: The Patriot Act

The Patriot Act and Illegal and Legal Electronic Warrantless Searches

Karen R. Watson [watsonk@ecu.edu](mailto:watsonk@ecu.edu)

East Carolina University

DTEC 6878 Spring 2007

### **Autobiographical Notes**

Karen Watson

Karen Watson is a Technology & Support Analyst at East Carolina University. She has worked in the Information Systems: Network Administration field for 5 years in Eastern North Carolina. Karen began working in networking in 2002 at WNCT-TV9 after graduating from the Networking Program at Pitt Community College. Karen was Cisco Certified Network Associate in 2002 and certified as a CompTia Network + Certified Professional in 2005. Karen also obtained an undergraduate degree in Business Administration from Barton College in Wilson, NC Karen continues to work in the Information Systems and business administration fields.

### **Abstract**

Since the signing of the Patriot Act after the terrorists' attacks of September 11, 2001, the U. S. Government has been accused of abusing the executive powers as they relate to the Patriot Act and the Illegal and Legal warrant less searches of average Americans. The accusations stem from illegally wiretapping average Americans' electronic communications, to violating average Americans' rights to privacy, to violating average Americans' rights to proper searches and seizures, and finally violating average Americans' civil liberties. To gain a better understanding of the Patriot Act, it will be defined as how it relates to electronic intercepting of communications, as how it relates to the three laws pertinent to wiretapping, as how it relates to the amendments to the rights to privacy as well as how it relates to the supporting facts of past governmental illegal and legal warrant less searches of electronic information. The supporting facts will be addressed from the laws, amendments, and articles. After researching to learn more about the Patriot Act in relation to Illegal and legal warrant less searches, there is undoubtedly facts that the government has performed Illegal warrant less searches on average Americans. Therefore, it would be beneficial for the average law-abiding Americans to protect their rights to privacy, civil liberties, et cetera by implementing cryptography on their networks.

### **Keywords**

Patriot Act, American Civil Liberties Union, Fourth amendment, Fifth Amendment, and Ninth Amendment , Pen Registers, Trap and Trace, Wiretap Statute (Title III), Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, civil liberties, Echelon,

## Introduction

The September 11, 2001 terrorists' attacks have influenced dramatic changes in the Patriot Act and the way the U.S. government handles and searches electronic information, devices, and hardware to protect Americans from future terrorists' attacks. The Bush Administration feels the changes made to the Patriot Act in 2001 helps to reduce the probability of future attacks in the U. S., but the American Civil Liberties Union (ACLU) feels the changes made to the Patriot Act helps the government secretly spy, eavesdrop, and evade the privacy and civil rights of Americans.

In the name of National Security, is it appropriate for the government to perform illegal searches of electronic information without warrants, or should the government make sure the proper warrants are in place to ensure the proper handling of executive powers and the privacy of Americans? For National Security, the government should take the necessary steps to counteract terrorism, but are these unwarranted searches in fact performed in the name of National Security? If time is of the essence, then yes, unwarranted searches should be allowed immediately, but any searches handled that do not threaten National Security should be checked and balanced to ensure the government is not abusing its executive powers.

In addition, an answer to the following question would be helpful, is the government unquestionably spying and eavesdropping on average American citizens? Certainly, it is quite possible the government is actually participating in unwarranted searches, eavesdropping on telephone calls, as well as recording conversations, et cetera; thus, intruding and invading the average Americans' civil liberties and rights to privacy. Conversely, unwarranted searches without systematic approaches and the proper checks and balances could impose on the civil liberties of Americans. Hence, understanding the Patriot Act, how it relates to electronic

interception of communications (wiretapping), relates to the three major laws of intercepting electronic information, and relates to the amendments considered to the rights to privacy will help to determine if the government is performing illegal or legal searches with proper checks and balances to protect the privacy and civil liberties of average American citizens.

### **The Patriot Act**

In order to get a better understanding of illegal and legal warrantless searches, it is important to discuss the Patriot Act and the major contents of the Patriot Act in relation to the surveillance of electronic communications (wiretapping). The terrorists' attacks of September 11, 2001 have caused the government to sign into law The USA Patriot Act on "...October 26, 2001..." and hence, use this act to help in the fight against the war on terrorism according to the Bush Administration (Gerdes, 2005). In Gerdes book, The USA Patriot Act or "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 'was signed into law by President George W. Bush 45 days after the terrorists' attacks'" (Gerdes, 2005). The USA Patriot Act encompasses many legislature laws but for the purposes of this paper, the discussion of interception of electronic communication (wiretapping) in regards to legal and illegal warrants performed by the government. The USA Patriot Act has helped to increase the government's executive powers and the monitoring and capturing of electronic information especially in regards to the Internet and other rapidly evolving technologies (The USA Patriot Act, 2005, p.4). Most importantly, the USA Patriot Act of 2001 has amended the three major laws in reference to electronic interception that will be discussed in the next section.

### Three Major Laws in Reference to Electronic Interception of Communications

The three major laws pertinent to the surveillance and capturing of electronic information are Title III (Wiretap Statute), Electronic Communications Privacy Act, and The Foreign Intelligence Act, which the USA Patriot Act has amended also. The first law is the Title III law. The following quote from The USA Patriot Act, 2005 article details the specifics of the Title III law.

Title III governs [sic] the contents of communications, defined as any information concerning the substance, purport, or meaning of that communication.’ The Supreme Court has held that the contents of a communication are entitled to full Fourth Amendment protection. Therefore, the government’s access to content information is limited by constitutionally imposed search and seizure requirements. In order to abide by these constitutional restrictions, Title III imposes strict limitations upon the government’s ability to obtain communication content:

- a law enforcement agency may intercept content only pursuant to a court order issued upon findings of probable cause to believe that
  1. an individual is committing one of a list of specifically enumerated crimes,
  2. communications concerning the specified offense will be intercepted, and
  3. ‘the pertinent facilities are commonly used by the alleged offender or are being used in connection with the offense.’
- Only designated officials can authorize such interception,
- The interception is authorized for a limited time period.
- Interception is subject to a statutory exclusionary rule: any information intercepted in violation of the wiretap statute cannot be admitted into evidence in any judicial or administrative proceeding (THE USA Patriot Act, 2005, pgs. 4 and 5). ”

The former specifications of the Title III law place the necessary safeguards in effect so illegal searches are not performed without first, probable cause, second, judicial court order, third, designated officials, and fourth, specified times. This law further specifies the place searched and the proper items seized during the search. A search of this magnitude would be classified as a legal search because there are no violations of American citizens’ civil liberties, or rights to

privacy. The second major law is the Electronic Communications Privacy Act (ECPA), which the government uses to intercept electronic communications to help monitor and capture information.

The ECPA details the surveillance of “...email and other electronic communications...” and the government’s access to this type of information (The USA Patriot Act, 2005, p.4). One difference between the Wiretap Statute and the ECPA is probable cause. The ECPA does not mandate probable cause. Furthermore, the use of trap and trace and pen register devices could pose serious privacy violations in this Act. According to Gerdes in the book, “The Patriot Act,” a trap and trace device is defined as “a device [sic] which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted” (2005, p.119). Also Gerdes, defines a pen register as “a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached” (2005, p.119). The biggest differences between the two surveillance devices is the trap and trace tailors to electronic communication and the pen register better covers telephone communications (Gerdes, 2005, p.119). More importantly, information obtained from trap and trace or Pen Registers devices can only be relevant during court proceedings when an attorney provides a judicial certification before the installation (The USA Patriot Act, 2005, p. 5). The third major law the government uses to intercept electronic communications is the Foreign Intelligence Surveillance Act (FISA).

Under the FISA Act, the government can obtain a court order to use electronic surveillance on any person guilty of acting as a foreign power or an agent of a foreign power in the United States including Americans (The Patriot Act, 2005, p. 5). The former actions of the

foreign power constitute the government's probable cause to use electronic surveillance. The ECPA as well as the FISA does not protect against privacy laws to the likes of the Wiretap Statute or Title III Act. The FISA, "...which applies primarily to the government's power in foreign intelligence and counter-intelligence cases; in short, does not offer many of the protections required under the Wiretap Statute" (The Patriot Act, 2005, p. 5). According to the ACLU, the pen register and trap and trace devices monitor all electronic communication ("originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source or a wire or electronic communication" Patriot Act, 2005, p.5) and to perform this type of surveillance the government only needs to show probable cause.

The Electronic information captured by government officials could include e-mails, web page downloads, and all other electronic information. Whereas before the passing of the Patriot Act, the use of the pen register and trap and trace devices were used to capture incoming and outgoing real-time communication on telephone lines only (The Patriot Act, 2005). The issue of the right to privacy occurs when the government illegally searches electronic information without obtaining a judicial court order as stated in the U. S. Constitution. These searches would constitute the definition of illegal search; thus, violating Americans' rights to privacy.

### **Amendments of the Rights to Privacy**

According to Ferrera, G., Lichtenstein, S. D., and Reder, M. 2004, the right to privacy is a "...penumbral or implied right, under the U. S. Constitution (p.258). The right to privacy considers "...the Fourth, Fifth, and Ninth Amendments to the U. S. Constitution ... and is supposed to help protect Americans from "...unwarranted government intrusions.'" (Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W., 2004, p. 258). The Fourth Amendment consists of the following:

The right of the [sic] 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 (Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W., 2004, p.455).

In other words, the government would need a warrant, which specifies the boundaries of the search and seizure. Does this mean the government would then have the additional safeguards in place to protect the privacy and civil liberties of Americans? Unfortunately, this is not exactly the case today because the government only needs to prove there is probable cause that you may be a person of interest in suspected terrorist activity or association, or involved in illegal activities. The Patriot Act's legislative law governs and allows the government to search and seize items such as belongings and electronic information pertinent to criminal investigations without any judicial restrictions and checks and balances to counteract terrorism. For example, suppose you were writing illegal numbers, et cetera in the state of N. C. and you were also laundering money outside the U. S. for whatever purposes you saw necessary. If the U. S. Government feels you are a threat to the National Security, an illegal search would be necessary to rule out suspected terrorist association or activity. Then, the government would use pen registers and trap and trace devices to monitor electronic communication, but would this type of illegal search be necessary on an average American computer user? Some Americans have mixed thoughts in reference to the government's eavesdropping on the average computer user.

According to the article "Presidential Powers, NSA Spying, and the War on Terrorism: Americans' Attitudes on Recent Events – Overview (2006)," a survey was performed by Belden & Russonello & Stewart for the ACLU, which revealed that 59 % of the voters wanted Congress to demand that illegal eavesdropping be eliminated, while the other 39% had no problems with eavesdropping as long as it protects the U. S. Additionally, the survey also revealed voters

strongly disapproved of searching homes (77%), torturing prisoners (65%), reading mail and e-mails (62%), secretly listening to phone calls with no warrants (55%), obtaining individual's library records (47%), holding prisoners at Gitmo with no lawyer or charges (35%), and surveillance of protesting organizations (24%). The results from the survey are important because it reveals how Americans view the fight on terrorism, illegal eavesdropping, and the abuse of executive powers of the Patriot Act. The results also show how Americans' attitudes are in reference to the President ordering illegal warrantless electronic searches with the checks and balances in place.

The former amendment helps to enhance the discussion of the next amendment pertaining to the right to privacy, the Fifth Amendment. For the purposes of the research paper, the specifications of the Fifth Amendment are brief, but are necessary in regards to the right to privacy. The Fifth Amendment, which supports the facts of how to care for detainees and their rights of due process and further specifications, consists of the following:

No person [sic] shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy or life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation ( Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W., 2004, p. 455).

In other words, everyone should have a fair representation in court and should not be prosecuted twice for the same crime, have property, liberty, or life neither taken, nor required to testify against himself without "...due process of law or without recompense (Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W., 2004, p. 455).

Finally, the last Amendment considered in the right to privacy is the Ninth Amendment, further specified below consisting of the following:

The enumeration [sic] in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people (Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W., 2004, p.456).

This amendment creates the kind of right to privacy. Again, the right to privacy considers the Fourth, Fifth, and Ninth Amendments as “.....the U.S. Constitution as applied to the states by the Fourteenth Amendment (Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W., 2004, p.258). In addition, the Fourteenth Amendment plainly states the no persons shall have deprivation of neither life or liberty, nor jurisdiction according to residence, nor due process of law without equality of the U.S. laws.

### **Government illegally eavesdropping on Average Americans**

Have you heard about Echelon? In an article written by Joseph Fitchett entitled “No Monopolies on Government Eavesdropping,” he writes about the U.S. government and how the European Parliament has discovered that the U.S. is indeed tapping private electronic telephone calls and has finally admitted to doing this (Fitchett, Joseph, 2000, p.1). Also, he writes about the Echelon system, which is considered the largest electronic database that records up to “2 billion telephone messages daily” is used to eavesdrop on private conversations instead for “... military and political antagonists” (Fitchett, Joseph, 2000, p.1). Further, the European Parliament believes that Washington is ready “to advance to U.S. hegemony in power and business.” Additionally, unknown sources said that it was nothing new for Washington to eavesdrop on private conversations and other countries participated in eavesdropping as well.

Moreover, in another article written by Kurt Nimmo entitled “What’s new about government eavesdropping? Critics of NSA (National Security Agency) surveillance the Echelon electronic database is discussed further (2006, p.1). The article confirms that the NSA has “‘Echelon’, the largest snooping database” in the world. “Echelon” is essentially a “monitoring

system, which consists of satellite interception stations in participating countries. The stations collectively monitor millions of voice and data messages each day.” Supposedly, this database monitors “telephone, e-mail, and web traffic” on typical Americans, but according to the government, it is primarily used to identify terrorist activities. In addition, the government has collaborative help of three “multinational telecoms, which are AT & T, Verizon, and Bell south (Nimmo, Kurt, 2006, p.1). It is apparent that the former telecom companies are “working under contract with NSA” (Nimmo, Kurt, 2006, p1).

Kurt Nimmo further writes that the government uses the Echelon database for “dictionary searches” for keywords like “terrorist” and or “drugs,” but when “the House on Committee on Intelligence requested that the National Security Agency and the Central Intelligence Agency provide a detailed report to Congress explaining what legal standards were used to monitor the conversations, transmissions, and activities of American citizens. There were no “legal standards, “ which pose concerns for Americans and violate the “Fourth Amendment of the Constitution” (Nimmo, Kurt, 2006, p.1). The article is valuable because Mr. Nimmo supports the idea that ACLU has purported from the beginning that “Echelon,” is a snoop database used to spy on average Americans. If according to Mr. Nimmo, the European Parliament in 2001 urged their citizens to incorporate cryptography on their networks, it would also benefit Americans to do likewise.

To further support, the concept of eavesdropping by the government, Suzanne Goldenburg, describes the events around the Bush in 2005 when President George Bush signed a “secret order in 2002 authorizing the NSA to monitor the international phone calls and e-mails of hundreds, if not thousands of U. S. Americans without obtaining a court warrant” in an article entitled “Senate refuses to extend Patriot Act amid eavesdropping row”(Goldenburg, Suzanne,

2005, p.1). Some people believe this was illegal and abused the civil liberties of the American people. Again, in contrast, President Bush felt he was operating within the law and his sole purpose should be to protect the American people. In fact, President Bush was quoted saying, "After [sic] 9/11 I told the American people I would do everything in my power to protect the country within the law, and that's exactly how I conduct my presidency" (Goldenburg, Suzanne, 2005, p.1). Since the Senate felt President Bush was unlawfully eavesdropping on Americans, the Senate refused to extend the Patriot Act provisions on Dec 16, 2005.

Additionally, Suzanne Goldenburg's article helps to prove that President Bush was eavesdropping on Americans without aligning with the provisions of the Patriot Act, which clearly state there should be a court order obtained before NSA can eavesdrop on Americans. In addition, some NSA officials did not participate in the wiretapping processes because they were concerned about the legalities of it. More important, the two following statements by Kate Martin, Director of the Centre for National Security Studies, summarizes the president's actions perfectly "The [sic] president apparently believed that he could order government officials to commit a crime, and if that's the case then it is astounding and frightening incident of lawlessness. We know that some in the justice department had advised the president that he was above the law when it came to national security, but we did not know the president had adopted that view himself and acted on it"(Goldenburg, Suzanne, 2005, p.1).

### **Conclusion**

In summary, the understanding of the Patriot Act, how it relates to electronic interception of communications (wiretapping), how it relates to the three major laws of intercepting electronic information, and how it relates to the amendments considered to the rights to privacy will help to determine if the government is performing illegal or legal searches with proper checks and balances to protect the privacy and civil liberties of average American citizens. In addition, the detailed discussion of the laws and amendments were relevant and equally important for the support of this paper, but the articles have certainly increased awareness of the certainties and possibilities of electronic eavesdropping by the U. S. government.

At any rate, the American people do not have the authority to stop the government from snooping, but as “average Americans,” we do have the right to protect our Constitutional Rights to Privacy. Therefore, it would be beneficial for law-abiding American citizens to use or “... incorporate [sic] cryptography on their network...” to protect their electronic information as the European Parliament urged their citizens to do.

## References

- Cauley, Leslie. (2006, May 10). NSA has a massive database of Americans' phone calls. *USA Today*. Retrieved on March 21, 2007 from,  
[http://www.usatoday.com/news/washington/2006-05-10-nsa\\_x.htm](http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm).
- Elder, Janet and Nagourney, Adam. (2006, Jan 26). New Poll Finds Mixed Support for Wiretaps. *The New York Times*. Retrieved March 08, 2007 from,  
<http://www.nytimes.com/2006/01/27/politics/27poll.html?ex=1296018000&en=d6f80e2c8cced000&ei=5090&partner=rssuserland&emc=rss>
- Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W. (2004). *Cyber Law*. West Legal Studies: Business, Thomson.
- Fitchett, Joseph. (2000, February 28). No Monopolies on Government Eavesdropping.” *International Herald Tribune* Retrieved on March 17, 2007, from,  
[http://www.iht.com/articles/2000/02/28/spy.2.t\\_2.php](http://www.iht.com/articles/2000/02/28/spy.2.t_2.php)
- Gerdes, L. (2005). *The Patriot Act*. Greenhaven Press: Farmington Hills, MI.
- Goldenburg, Suzanne. (2005, December 17). Senate refuses to extend Patriot Act amid eavesdropping row.” *Guardian Unlimited Special Reports*. Retrieved March 17, 2007 from <http://www.guardian.co.uk/usa/story/0,12271,1669540,00.html>
- Government Eavesdropping. Retrieved on March 18, 2007 from,  
<http://www.cnn.com/interactive/allpolitics/0512/explainer.eavesdropping/frameset.exclude.html>
- Kopel, D. & Thompson, D. Government Eavesdropping via E-mail. (1999, July 4). *Dave Kopel*. Retrieved on March 17, 1007 from,  
<http://www.davekopel.com/DigitEcon/OpEds/Government-Eavesdropping.htm>

Nimmo, Kurt. (2006, May 12). What is new about government eavesdropping? Critics of NSA surveillance forget a long and ongoing history of international surveillance. Retrieved on March 21, 2007 from,

[http://gmn.tv/headlines/9074/What\\_s\\_new\\_about\\_government\\_eavesdropping](http://gmn.tv/headlines/9074/What_s_new_about_government_eavesdropping)

Presidential Powers, NSA Spying, and the War on Terrorism: Americans' Attitudes on Recent Events – Overview. (2006, Feb24). *American Civil Liberties Union*. Retrieved March 09, 2007 from,

<http://www.aclu.org/safefree/nsaspying/24262res20060224.html>

Scheuerman, William E. Emergency Powers. (Dec. 2006). *Annual Review of Law and Social Science*. Vol. 2 256-277

<http://arjournals.annualreviews.org.jproxy.lib.ecu.edu/doi/pdf/10.1146/annurev.lawsocsci.2.061206.074644>

*The USA Patriot Act*. (2005, November 17). Retrieved on March 17, 2007 from,

<http://www.epic.org/privacy/terrorism/usapatriot/>