March 2010

Internet Privacy in the United States

Jesse P. Bassett
Worcester Polytechnic Institute

Kara Buckley
Worcester Polytechnic Institute

Project Number: 123-456-789

An Examination of Internet Privacy in the United States

An Interactive Qualifying Project

Submitted to the Faculty of

Worcester Polytechnic Institute

in partial fulfillment of the requirements of the
Degree of Bachelor of Science

Submitted by:

Jesse Bassett _____

Kara Buckley _____

Date: March 4, 2010

Submitted to:

_____

Professor Kent J. Rismiller

Abstract

The main goal of this project is to reflect upon the history of Internet privacy laws, examine the current balance of privacy vs. security in the United States, and postulate possible corrections to help the balance. This will be done through the inspection and criticism of past privacy laws, and the investigation of the solutions comparable countries have come up with.

Contents

1 Introduction

America has a long precedent of protecting the privacy of its citizens from each other as well as the government itself. Tort law covers defamation of character, and the Fourth Amendment provides protection from search and seizure of physical property, but the advent of the Internet has changed the way these laws can be applied. The Internet is not a physically tangible entity, nor is anything that resides within it, and lawmakers have been struggling to adapt the aging legal code to cope with this.

The laws to protect citizens from search and seizure are well defined. They were first established by the Fourth Amendment, in the Bill of Rights. However, these protections were designed for a material world, and in the digital world of the modern age, these protections hold less meaning. Determining privacy on the Internet is a difficult task, due to the relatively young age of the technology. It is much easier to conclude that someone drilling a hole in a fence to spy on their neighbor is a violation of personal privacy, as opposed to using a search engine to find their neighbors personal information on their Facebook or MySpace page. The legal code is adapting to changes like this, abstracting the concept of personal property.

However, private citizens are not the only residents of cyberspace. Governments have tried to control and monitor this new medium to the best of their abilities, and because of the lack of a firm definition of what is permissible online, many questions have been raised about the legality of government actions online. One of the duties of a government is to ensure the safety of its citizens, but also to respect their citizens privacy unless they have just cause. Although there are many well defined laws and precedents for how to handle invading a persons private life, the laws for monitoring private digital life are much more gray. While intercepting and reading a piece of posted mail is a tedious and

hard to disguise task, it is a simple and easy to read electronic mail, and it is almost undetectable as well. Great care has to be taken to ensure the safety of citizens, while still maintaining their privacy.

Each country has taken its own unique approach to adapting to this new age. America has looked to other countries in the past to help determine their next course of action. Due to this, the global reaction towards Internet privacy is important. Comparable countries, such as England and the European Union, could give the United States insight as to the best course of action to take. Because of the parallel laws and values between these countries, the United States can learn from their failures, and halt any analogous legislation that is being considered for implementation. Even more, the United States can see what plans succeeded, and take similar measures.

2 Background Materials

To be able to completely grasp Internet privacy laws, the privacy laws before the invention of the Internet must be understood, and applied to the new technology. Therefore, in-depth research was conducted on landmark precedent-setting acts, such as the Foreign Intelligence Surveillance Act and the Electronic Communications Privacy Act. Though neither act specifically refers to any new technology (both were passed before the '90's, and are therefore technologically outdated), they laid the groundwork for the spirit of Internet privacy, and have been interpreted to justify more recent laws, such as the Patriot Act, the Protect America Act, and the FISA Amendments Act.

FISA, the Foreign Intelligence Surveillance Act, was passed in 1978, and it allowed the government to electronically spy on foreign powers, or agents of foreign powers. FISA created FISC, the Foreign Intelligence Surveillance Court, which reviewed FISA orders and determined whether or not surveillance was to be conducted. To be allowed to hold surveillance, a federal intelligence officer had to show FISC several things, including how the suspect was to be identified, why the agent believed the suspect was an agent of foreign power, and what methods of surveillance, as well as what minimization procedures, were to be utilized (Addicott and McCaul, 2008). Additionally, the agent had to show that the primary purpose of the surveillance to be conducted was to acquire foreign intelligence information, not information about a criminal investigation. For the request to then be granted, the FISC judge must find probable cause that the target was knowingly participating in either clandestine or secret activities, or sabotage or international terrorism, on behalf of a foreign power, or was an accomplice to another who is conducting such activities. A granted request approved electronic surveillance for a certain amount of time; for agents of a foreign power, 90 days, and for a foreign power itself, a year (EPIC, 2007a). Upon

a granted request, the FBI was allowed to acquire business records, specifically records of transportation carriers, hotels, storage locker facilities, and vehicle rental agencies (O'Donnell, 2004).

ECPA, the Electronic Communications Privacy Act, was passed in 1986, and referred to slightly more current technology. ECPA prevented the government from intercepting electronic communications that were in transit, or that were stored on a network, but did not apply to public communications. Simply put, it protected e-mails from one individual to another, but not chat rooms with public postings. It went on to authorize roving wiretaps, which are basically wiretaps on an individual as opposed to a location. These roving wiretaps must be backed by a high-ranking Justice Department official, and could only be used when it was reasonable to believe that the target was near the communications facility being monitored (Kaas, 2002). Essentially, if a target used a public pay phone, the government agency could only monitor that specific pay phone if it were reasonable to believe the target were near the pay phone at the time of surveillance. Finally, it required "electronic communications services and remote computing services" to divulge a subscriber's name, address, phone number and billing records, types of services uses, and length of use, upon subpoena. Usually, this was only applied to traditional telephone communications, and did not encompass the Internet.

Neither of these acts directly mention the Internet, or any technology of the like, mainly because the acts were created before the development of the new technology. However, the influence of these acts on the more current legislation is indisputable. The legislators used these precedent-setting acts to aid in the creation of the later privacy acts, taking into account not only the language of the law but the spirit as well. They updated the language in accordance with the new technology, and edited the spirit of the law to match what the public

expected at the time.

The best example of an act passed to harmonize with public opinion is the USA PATRIOT Act. The USA PATRIOT Act, referred to as PA, is actually an acronym, which stands for United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. Immediately following the terrorist attacks of September 11, 2001, there was a widespread panic among American citizens; they were terrified about national security, and wanted drastic measures to ensure nothing of that caliber happened again.

The passage of the Patriot Act gave law enforcement officers and federal agents an exponential increase in power. Due to the epidemic of hysteria throughout the American public, people were willing to give up their Constitutional liberties to ensure their safety. What Congress had previously deemed "overly intrusive and possibly unconstitutional" was being granted, because the public believed their personal well-being was in danger (Evans, 2002). The public wanted stronger national security laws, and that was what the legislators passed.

The PATRIOT Act built off both of FISA and ECPA. It expanded FISA, changing the wording of the surveillance standard. Under PA, the collection of foreign intelligence no longer had to be the "primary" purpose of the investigation, but merely a "significant" purpose (EPIC, 2007b). Legislators understood that terrorists often committed crimes as well, and, under the previous statute, the government could only investigate one avenue at a time.

Furthermore, PA allowed separate branches of the government to communicate with one another. Before PA, separate branches of government agencies were prohibited from communicating with one another; any counterintelligence information learned during a criminal investigation could not be shared with a foreign intelligence agency, and vise versa. This measure allowed the various government agencies to work together to accomplish a common goal (Jonas,

2005).

PA went on to broaden the FBI's power to include the authority to request an order for any"tangible thing including books, records, papers, documents and other items, specifically education records, computer files, book purchases and library borrowing records" (O'Donnell, 2004). The regulations in place before PA stated the FBI needed to prove probable cause for their request to be granted. Under PA, the FBI could simply state the records might be associated with an ongoing investigation involving either terrorism or foreign intelligence activities (EPIC, 2007b).

It also elaborated on ECPA, broadening roving surveillance. Under the Patriot Act, roving surveillance was extended to cover computer equipment, and even authorized surveillance on third parties coming in contact with the suspect. Additionally, the subscriber records available via subpoena were increased to include"records of session times and durations, any temporarily assigned network addresses, and the means and source of payment for such service of a subscriber (including any credit card or bank account number)" (Lee, 2003) .

The PATRIOT Act was not the last act passed regarding Internet privacy. In fact, PA affected the later legislation, due mainly to the fact that it was so controversial. Once the dust settled, the American public realized the liberties they had sacrificed in accordance with PA. Many of the sections of the Patriot Act were scheduled to sunset at the end of 2005; some sections were renewed, others were not. Regardless, it became apparent that the current privacy laws in place were not going to last. The changing technology, as well as the changing public opinion, needed to be accounted for.

PAA, the Protect America Act, was passed in 2007 in an attempt to update past acts, specifically FISA, to keep legislation up to date with technology. Supporters of PAA argued that the terminology in FISA was outdated, and was

inadvertently preventing foreign intelligence officers from collecting intelligence on foreign agents located outside the country. To rectify this, the wording of FISA was amended: what constituted"foreign intelligence" in FISA maintains constant in PAA, but the definition of electronic surveillance is adjusted. PAA states that what was considered to be electronic surveillance under FISA is not electronic surveillance if it incorporates surveillance directed at a person reasonably believed to be outside the United States. This means that if surveillance is being conducted on someone thought to be outside the United States, they are not under the jurisdiction of FISA, and therefore warrants and court approval are not always required. PAA allows the president to approve of warrant-less surveillance for up to a year, given there are procedures to ensure the person watched is outside the United States, a communications service provider, custodian, or someone with access to communications assists in obtaining the information, and that a significant purpose of the operation is to obtain foreign intelligence information (Cardy, 2008). Under PAA, American citizens felt they had more personal privacy, and that only the liberties of foreign nationals would be infringed upon.

Finally, the FISA Amendments Act, or FAA, enacted in 2008, is directly based on FISA, and makes some significant changes to the original version. Under this act, the federal government cannot intentionally spy on anyone known to be in the United States, nor a United States citizen located outside the United States. Even more, it specifically prohibits reverse targeting, or watching someone outside the United States to gain information about a suspect located within the United States. However, in the original text of FISA, the target explicitly had to be either a foreign power or an agent of a foreign power. In the FISA Amendments Act, there is no such requirement; it merely states the target must be a foreigner reasonably believed to be overseas (Blum, 2009).

The FISA Amendments Act also differentiates between entirely foreign communications routed through the United States, and international communications; no warrant is necessary for the former, while the latter is subject to FISC oversight. While it does not reference which technology specifically is to be surveilled, it does require the government get the information with the assistance of an electronic communications service provider. The Amendments Act also provides for telecommunications providers, granting them immunity and allowing them to challenge the legality of such a government order via FISC (Blum, 2009).

This act is the first to include serious federal oversight, requiring each government agency to report to Congress and FISC annually, to ensure their cooperation with the each clause of the act. The inclusion of this specification shows the American public's suspicion in the government, and unwillingness to trust each government agency to monitor itself. Each government agency has to report not only to the Director of National Intelligence and the Attorney General, but Congress and FISC as well. The reports must include the use of the information obtained, how much information gathered concerned an United States citizen, and the number of targets later proved to be in the United States when communications were being monitored. Furthermore, the Attorney General and the Director of National Intelligence must assess government compliance with targeting and minimization procedures every six months. Then, they must report to Congress and FISC, detailing all proceedings before FISC, any targeting and minimization procedures put in place recently, and any incidents of discord with procedures by any office (Blum, 2009).

FISA, ECPA, PA, PAA, and FAA are the major precedent-setting acts involving Internet privacy throughout the history of American privacy law, and represent the changing trend in privacy law in America. However, America has

not been alone in struggling to find a balance online. The European Union has also attempted to solve this delicate situation. They introduced a directive in 2002 in order to more unify the provisions of the Member States (Art.1(1) European Union, 2002, p. 42). Among its provisions, it required telecommunications companies to erase or make anonymous any data it may have about the traffic it transported, as soon as it was no longer critical to the transmission that the data be saved (Art.6(1) European Union, 2002, p. 44). However, in 2006, in response to the Madrid train bombings in 2004, a new directive was drafted that overturns a number of these articles.

The goal of this new directive is to strengthen the powers of the governments over the Internet, allowing them to use data collected from electronic communications. It requires that the telecommunications industries retain the data for six months up to two years (Art.6 European Union, 2006, p. 58). Recorded data includes call logs from telephone conversations, IP address and E-Mail connection information, and even the location of a mobile phone call (Art.5(1) European Union, 2006, p. 57-8). Each country was given until March 15, 2009 to enact the Directive, but few actually had by that time. Denmark has enacted the full extent of Directive 2006/24/EC, and the United Kingdom currently has a bill passing through Parliament that would carry out the Directive (OPSI, 2009).

This is not the United Kingdom's first attempt to monitor its citizens. Immediately after the terrorist attacks on September 11, 2001, Parliament rushed through a bill very similar to the USA-PATRIOT Act in America. The Anti-Terrorism, Crime and Security Act of 2001 (OPSI, 2001) similarly empowered law enforcement, giving them extended reach and powers. The Secretary of State was given the power to create"...a code of practice relating to the retention...of communications data..." (Pt.11(102)(1) OPSI, 2001). The following

sections gave him the power to request any communications provider, or group thereof, to hold retain data for as long as he requests (Pt.11(104)(3) OPSI, 2001).

Internet privacy is an issue that has constantly taken up a portion of the world stage for many years. Legislators are even now trying to find the delicate balance between Internet privacy and Internet security. The medium of the Internet is simply too new to be completely understood by lawmakers, and it will take some time before there is a complete grasp.

3 Research Methods

At WPI, no IQP or MQP has ever been conducted on this precise topic. Several past projects have been conducted on file-sharing, and the legal ramifications thereof, but none have expanded past basic copyright law. However, the issue of privacy in the digital domain has moved into the foreground of the legal issues facing the 21st century. As such, this paper will be devoted to evolution Internet privacy laws and regulations in the United States, as compared to other countries around the world.

Historical analysis will play a major role in understanding the previous steps that American litigators have taken. Prior attempts to adapt American privacy laws to the Internet will be examined, and critiqued to determine degrees of success. Past measures will also be compared to similar attempts made by foreign countries, to show the global tide towards Internet privacy. An in-depth analysis will then be utilized in an attempt to find the causes of the problems that have arisen over time.

Research will be conducted on precedent-setting legal action, both in the United States justice system and those in other nations. Case studies will be performed on specific cases, including cases challenging the constitutionality of any ground-breaking acts discussed, as well as any cases involving either increasing or decreasing the personal privacy of an individual citizen on the Internet. Likewise, cases encompassing similar topics from comparable countries will be subject to case studies.

Due to the in-depth nature of the legal research that will be conducted, there are few pertinent physical resources available at the school library. The majority of the available materials are either in digital form in the library databases, or online. Additionally, law journals from across the nation are invaluable resources; many articles have been published on parallel topics, and contain not

only summaries of legal precedents, but specific cases that could be further researched. Moreover, being inside the United States makes obtaining legal documents from other countries more difficult. The language barrier is only the first problem, often coming coupled with foreign disclosure policies. Access to these materials in a physical form is almost impossible, and research therefore must be conducted online. Due to the sensitive nature of the legal materials, the main sources for these are activist sites like OpenNet Initiative, or humanitarian organizations, such as Reporters Without Borders.

With regards to the topics of discussion, the project will commence with the review of older privacy laws and regulations in place before the introduction of the Internet. The previous privacy laws and regulations before the digital age must be completely understood, in order to attempt to apply the outdated laws to the current technology. The precedents set before the digital age, such as the Foreign Intelligence Surveillance Act and the Electronic Communications Privacy Act, are still valid, and must be applied to the ever-changing technology.

An in-depth analysis of the past laws and regulations will show the advancement of the privacy laws over time, culminating in the dissection of current laws and regulations in effect. Taking a look at the controversies surrounding the past major acts of legislation, such as the Patriot Act and the Protect America Act, and showing how the current laws were affected by the past controversies, will show how these laws evolved according to what the public expects of privacy laws.

Delving into how other civilized countries are handling the same issue will give an idea of what alternative paths there are to dealing with this issue. The reaction of analogous countries like England and groups like the European Union to the digital age will be similar to the reaction of the United States, and appraising their privacy law, and the controversies and successes of these laws

will give a glimpse of what the United States may still do to adapt to this new technology.

4 Internet Privacy in the United States

Before being able to critique the laws governing Internet privacy, one must fully understand what each law does. The following section is devoted to just that. Each law is explained in full detail, to provide a complete comprehension of the law. Once one is aware of the laws and their meanings, the laws can be analyzed to determine their effectiveness.

4.1 Foreign Intelligence Surveillance Act—FISA

The first real act that affected Internet privacy was the Foreign Intelligence Surveillance Act of 1978, better known as FISA. FISA was groundbreaking because it allowed the President, acting through the Attorney General, to authorize warrant-less electronic surveillance, given the surveillance was for foreign intelligence purposes (US Senate, 1978). FISA was designed to make it easier to get approval for electronic surveillance aimed at foreign powers, as evident by the specific provision of the Act including a significant purpose of any electronic surveillance is to obtain foreign information. However, any evidence obtained through electronic surveillance would not be excluded from criminal proceedings (Kaas, 2002).

The main purpose of FISA was to create an act to govern the gathering of foreign intelligence. Between 1975 and 1976, the Church Committee researched the practices of domestic spying, and found severe government abuses. The Committee discovered 500,000 FBI investigations into "alleged subversives" from 1960 to 1974. Additionally, the Committee learned that the CIA had been participating in the widespread practice of opening mail of United States citizens. Furthermore, the Army was also abusing its power, holding secret investigations into 100,000 United States citizens, merely because they were against the

Vietnam War. Finally, the NSA oversaw every international cable going to or coming from the United States from 1947 to 1975, and were holding surveillance of telephone conversations of 1680 United States citizens. The blatant abuse of civil liberties prompted Congress to introduce and pass FISA, which was directed to "provide a statutory framework for the U.S. government to engage in electronic surveillance and physical searches to obtain 'foreign intelligence information" (Blum, 2009).

FISA was introduced by Senator Edward M. Kennedy (D-MA) in 1977, with nine senators cosponsoring the bill (Senators Birch Bayh (D-IN), E.J. Garn (R-UT), Daniel K. Inouye (D-HI), John L. McClellan (D-AR), Strom Thurmond (R-SC), James O. Eastland (D-MS), Walter Huddleston (D-KY), Charles McCurdy Mathias, Jr. (R-MD), and Gaylord Nelson (D-WI)). The final version of FISA passed the Senate on April 20, 1978, with a vote of 95 to 1, and the House on October 12, 1978 with a vote of 266 to 176. President Carter signed it into law on October 25, 1978.

FISA created two courts, the Foreign Intelligence Surveillance Court, referred to as FISC, and the Foreign Intelligence Surveillance Court of Review, or FISCR. FISC was a secret court, made up of seven non-disclosed federal district court judges, each serving seven years terms. Each judge had jurisdiction to grant applications for electronic surveillance anywhere within the United States. FISCR was also a secret court, though it was made up of three non-disclosed either federal district or federal appellate judges. The purpose of FISC was to review any appeals due to application denials made by FISC. The judges from FISC and FISCR were chosen by the Chief Justice of the Supreme Court (Addicott and McCaul, 2008).

Applications for electronic surveillance were submitted to any FISC judge for approval. Each application for electronic surveillance had to meet several

requirements; a certain set of information was required for the application to be approved. First, the name of the officer or agent submitting the application must be given and they must have the Attorney General's approval to submit the application. Next, the identity of the target of surveillance, if known, must be given, along with the reasoning as to why the officer believed the suspect was a foreign power or an agent of a foreign power. Additionally, a specification of what kind of information was attempting to be obtained must be stated, and why said information could not be accessed through normal investigations. Finally, the application must state how long surveillance will be planned for, and what minimization procedures will be used, meaning what procedures will be implemented to ensure little intrusion into a United States citizens privacy. (US Senate, 1978)

The judge must examine the application to determine whether or not to grant it. For an application to be granted, all the information supplied must meet the requirements. Moreover, there must be probable cause that the suspect is a foreign power or an agent of a foreign power, and that the target is either at the facilities to be watched, or is about to be there (EPIC, 2007a). Also, the judge must take into account if the suspect lives in the United States and if so, that the application is not submitted solely due to actions that are protected under the First Amendment (Addicott and McCaul, 2008). After considering all this, the judge can either give an ex parte order as petitioned, modify the application, or deny it entirely. If all conditions are met and the judge approves the application, surveillance is allowed for ninety days, or however long is necessary to accomplish its purpose. Extensions of orders are allowed, given the application for extension is filed through the same channels as the original application. (US Senate, 1978)

Additionally, the Attorney General can, in an emergency situation, autho-

rize electronic surveillance, given a judge is immediately informed of the authorization, and an application is made within twenty-four hours. However, the president can, through the Attorney General, authorize emergency electronic surveillance for up to fifteen days, given it is during a Congressionally declared war. Normally, without a judicial order, surveillance must be stopped when the information pursued is retrieved, the application is denied, or twenty-four hours has passed. It does not allow the use or disclosure of information involving any United States person that was obtained through emergency-granted electronic surveillance that was disallowed, unless the person consents. It does, however, allow such information to be used to protect the life or safety of a person, given the Attorney General's approval. (US Senate, 1978)

FISA also set up procedures to ensure power was not abused. The Attorney General was required to submit an annual report to the Administrative Office of the United States Courts and to Congress. The report must state the number of applications made as well as the number of applications for extensions, along with how many applications were approved, modified, or denied. Moreover, twice a year the Attorney General must apprise the House and Senate Committees on Intelligence of any electronic surveillance conducted. Finally, these Committees must report every year, for five years, to the House and Senate, making recommendations (US Senate, 1978).

4.2 Electronic Communications Privacy Act—ECPA

The next act affecting Internet privacy is the Electronic Communications Privacy Act of 1986, or ECPA. ECPA was basically an attempt to update the existing laws to keep up with the evolving technology. The act was Congress' way of weighing what law enforcement needs to be effective, versus the privacy rights afforded in the Fourth Amendment. The overall goal of ECPA was

to regulate government access and interception of the new modes of electronic communications, when either stored or in transit. (Kaas, 2002)

ECPA was introduced by Rep Robert W. Kastenmeier, on June 5, 1986. There were 35 cosponsors to the bill. The final version passed the Senate by voice vote on October 1, 1986, and the House unanimously approved the Senate Amendments, by voice vote, on October 2, 1986. President Reagan signed it into law on October 21, 1986.

ECPA broadened Title III of the Omnibus Crime Control and Safe Streets Act of 1968, referred to as the "Wiretap Act." The original act protected "wire or oral communications", stating surveillance was allowed only under a judicially-approved order, which had to meet even higher specificity standards than normal Fourth Amendment warrant requirements. ECPA extended the original "wire or oral communications," replacing it with "wire, oral or electronic communications" (The Wiretap Act and ECPA). Specifically, the electronic communications covers e-mail communications in transit, but not Internet chat room communications. The act distinguishes between e-mail and chat rooms, arguing that e-mails have an expectation of privacy while chat rooms do not; the chance of e-mails being read by anyone other than the specific recipients is slim, while chat room postings are for the entire public to see. (Kaas, 2002)

The second part of ECPA is referred to as the Stored Communications Act, and it limits the power of the government to force a third party, specifically an Internet service provider (ISP), to turn over content and non-content information. Basically, to access any unopened e-mail stored by an ISP for 180 days or less, a regular Fourth Amendment warrant stating probable cause is required, not the more stringent warrant necessary for e-mail in transit. For any unopened e-mail stored by an ISP for more than 180 days, only a court order or subpoena is required, at a significantly lower standard than probable

cause. However, opened e-mails, regardless of how old they are, also only require a court order or subpoena. Under ECPA, the government can subpoena ISPs to "reveal a subscriber's name, address, phone number and billing records, the types of services used, and the length of use" (Lee, 2003).

This act was groundbreaking, due to how personal information held by a third party was normally interpreted. Originally, the Supreme Court had stated the Fourth Amendment does not apply to any personal information voluntarily disclosed to a business, and the government could access any information given to the business without the Fourth Amendment warrant requirements. Without this act, any e-mails held by ISPs would be considered voluntary information given to a business, and the government would be able to access e-mails through the ISP with little to no cause.

Additionally, ECPA provided for the power of law enforcement to conduct roving wiretaps, which is essentially a wiretap on a person as opposed to a specific location. For a roving wiretap application to be allowed, it has to show probable cause that the target's elusive actions could prevent the interception of any pertinent communications from a specific location, making a conventional warrant ineffective, and it must also be approved by a high-ranking Department of Justice official. Furthermore, the roving wiretap can only be applied to locations when the law enforcement officers have reason to believe the target will be near said location. (Kaas, 2002)

Finally, it created the "Pen/Trap statute," which regulates pen registers and trap and trace devices. A pen register basically just records the numbers dialed on a specified telephone. A trap and trace device keeps track of how many times the specified telephone calls each number. For the application for a pen register or trap and trace device to be approved, an agent must certify that the information to be collected is pertinent to an ongoing investigation. However,

the statute expressly states that no communications content can be gathered, meaning an approved application for a pen register or trap and trace device is not grounds to listen to the actual conversation.

4.3 Communications Assistance for Law Enforcement Act — CALEA

The Communications Assistance for Law Enforcement Act, better known as CALEA, was passed in 1994. At the time, the technology available to the general public was cutting edge. However, the surveillance technology had not caught up to the ever evolving technology used in day-to-day life. As such, the surveillance technology was not always compatible with the technology used by the general public. This act was an attempt to rectify that.

CALEA was introduced by Rep Don Edwards (D-CA), and was cosponsored by Rep Henry J. Hyde (R-IL). It was introduced into the House on August 9, 1994, and an amended version passed on October 5, 1994 by voice vote. The amended version passed the Senate without further changes on October 7, 1994, also by voice vote. President Clinton then signed it into law on October 25, 1994. (US House of Representatives, 1994)

As previously stated, the main purpose of CALEA is to ensure the surveillance technology is compatible with the technology the public is using. The act goes about this by forcing telecommunications carriers to make sure that all their "equipment, facilities, and services adhere to standards that enable law enforcement to pursue call intercepts, pen registers, and trap and trace technologies for surveillance" (US House of Representatives, 1994). Basically, CALEA puts the telecommunications carriers themselves in charge of ensuring the surveillance technology will be compatible with their technology.

Although CALEA gives guidelines on how to determine what qualifies as

a telecommunications carrier, it leaves it up to the Federal Communications Commission (FCC) to determine which specific providers classify as telecommunications carriers. CALEA states for the FCC to classify a provider as a telecommunications carrier, its "provision of 'wire or electronic communication switching or transmission service must be a replacement for a substantial portion of the local telephone exchange service"' and it must be in the "public interest" to classify the provider as a telecommunications carrier (US House of Representatives, 1994). However, any provider engaged in "generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications" is specifically exempt (US House of Representatives, 1994).

The FCC followed the guidelines dictated by CALEA, and created a specific three-prong test from said guidelines. First, the provider must implement a transmission or switching function. Next, the providers must take the place of a considerate amount of local telephone exchange service. Finally, it has to be in the public's best interest to qualify the provider as a telecommunications carrier. Under this test, the FCC found Broadband Internet Access Services and VoIP (interconnected voice over Internet Protocol) Services to be considered as telecommunications carriers.

Finally, CALEA requires the telecommunications carriers to be able not only to implement surveillance, but to separate the information. It requires providers be able to separate the communications of an individual users from the network. It also requires providers be able to separate the content information from the non-content information of a specific user.

4.4 USA PATRIOT Act

The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, commonly referred to as the PATRIOT Act but shortened to PA, was passed in 2001, in response to the terrorist attacks of 9/11. The Bush Administration's rough draft of the act was brought before Congressional leaders less than a week after the attack. The rough draft was debated for two weeks, and the final version was brought before the House of Representatives on October 2, and the Senate on October 4. The Senate took only eight days to approve the act, with a vote of ninety-six to one. The House took slightly longer, eleven days, with a vote of three hundred thirty-seven to seventy-nine. Congress passed the PATRIOT Act on October 25, 2001, and President Bush signed it into law the next day (Evans, 2002).

In this climate of panic and hysteria, personal privacy was exchanged for national security. The PATRIOT Act first modified the roving wiretaps allowed under ECPA, and began applying the FISA standards to roving wiretaps, as opposed to the stringent ECPA standards. It went on to broaden the power of roving surveillance, under Section 206, authorizing roving wiretaps to follow the target, and monitoring a third party, given they are "implicated as an accomplice of the target in circumstances where the Court finds that the actions of the target of the application have the effect of thwarting the identification" of the third party (Smith, 2003). Additionally, it extends rolling surveillance to computer equipment, allowing the search of third party e-mails. Furthermore, Section 206 says nothing about limiting surveillance to when the target can be reasonably presumed to be close to the communications device (Kaas, 2002). Finally, Section 225 provides immunity to the ISPs for assisting with FISA wiretaps. (Christensen, 2006)

The PATRIOT Act also broadens what information the ISPs must provide

under subpoena, to include "the records of session times and durations, any temporarily assigned network addresses, and the means and source of payment for such service of a subscriber (including any credit card or bank account number)" (Kaas, 2002). The main purpose of this inclusion was to ensure the true identity of the subscriber could be obtained, in the event the person registered under a false name.

Sections 212 and 217 basically allow ISPs to voluntarily disclose information to the government, without a court order or subpoena. Section 212 allows ISPs to share both content and non-content information, given there is a reason to believe there is imminent danger of physical injury or death if the information is not disclosed immediately. Section 217 allows ISPs to invite the government to wiretap communications involving hackers on their network. This section was designed to protect officers when they are given permission by the owner or operator, but specifies that the officer must be involved in an ongoing investigation, and must have a reason to believe the contents of the communication will relate to said investigation (Lee, 2003).

Section 215 expands what records the FBI can request under FISA, previously allowing "records of transportation carriers, hotels, storage locker facilities, and vehicle rental agencies." Under Section 215, it was expanded to include any "relevant 'tangible item (including books, records, papers, documents, and other items)"' (O'Donnell, 2004). Furthermore, it changed what was required for an order to be approved, from believing the target to be involved in terrorism and showing how the requested items would prove it, to stating the records are "'sought for' a foreign intelligence or terrorism investigation" (O'Donnell, 2004). Finally, Section 215 included a gag order, which prevented anyone who had knowledge of the requests to disclose the fact that the requests were sought.

Section 216 arguably allows for the most drastic expansion of government

surveillance. First, it expands the pen registers and trap and trace devices to include Internet surveillance, allowing the devices to track "dialing, routing, addressing and signaling information anywhere within the United States" (Lee, 2003). Under Section 216, for a pen register or trap and trace device to be placed, the government must state that the information likely gathered is "relevant to an ongoing criminal investigation," as opposed to the usual probable cause (Kaas, 2002). Additionally, the FBI is allowed to use a program known as Carnivore, which "monitors e-mails, web pages, chat rooms, and other signals on the network it is linked to" with the same standard applied (Kaas, 2002). However, the section states that any orders issued under it do not include orders for content, which means the pen registers and trap and trace devices can only reveal non-content information.

Though Section 218 does not deal specifically with ISPs or Internet surveillance, it is still pertinent to Internet privacy. Section 218 broke down the "wall" that existed between regular law enforcement and foreign intelligence agents. Previously, the two bodies were not allowed to communicate with one another, prohibiting the sharing of information. Under Section 218, any information gleaned from a foreign intelligence investigation could be shared with law enforcement, and used in criminal proceedings (Christensen, 2006).

The PATRIOT Act was a monumental act, with over 1000 sections. Due to the large size, and the short time spent reviewing each specific section, lawmakers set sunset provisions on the more controversial acts. Most importantly, Sections 206, 212, 215, 217, 218 and 225 were all set to sunset on December 31, 2005.

4.5 Protect America Act — PAA

The Protect America Act, better known as PAA, was signed into law in 2007. It was designed as a way to modernize FISA. The technology was growing faster than the laws in place, and legislators needed to update the existing laws to fit the developing technology. The Protect America Act was the solution to make the laws applicable to the new technology available.

The Protect America Act was introduced by Sen. Mitch McConnell (R-KY) on August 1, 2007, and cosponsored by Sen. Christopher S Bond (R-MO). The Senate passed an amended version on August 3, 2007, with a vote of 60 to 28, and the House passed the same version on August 4, 2007, with a vote of 227 to 183. President Bush signed it into law on August 5, 2007. (US Senate, 2007)

PAA came about after the scandal involving the Bush administration. In December 2005, the New York Times published reports about a program secretly approved by the president, that allegedly allowed warrantless domestic surveillance conducted by the National Security Agency (NSA). The program, referred to as the Terrorist Surveillance Program, or TSP, allowed NSA to monitor international e-mails and telephone calls, without the previously needed FISC approval.

The Bush administration and TSP supporters pointed out that evolving technology unintentionally extended FISA's reach to areas that were not originally intended to be protected by FISA. For example, under the wording of the original FISA text applied to current technology, the government was required to get a warrant to obtain "intelligence information against a target located overseas" (Cardy, 2008). Obviously, this was not the intended meaning of the original legislators, and it became apparent that FISA needed to be updated.

The Protect America Act changed several parts of FISA, but kept some the same. For example, what constitutes foreign intelligence in FISA remains

the same in PAA, with 'foreign' specifically applying to the content of the information, as opposed to the location it is obtained or the nationality of the informant. 'Foreign intelligence' still refers to "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against ... harms or clandestine operations against the United States" (Cardy, 2008).

However, PAA did redefine what was to be considered electronic surveillance. The act stated that surveillance aimed at someone "reasonably believed to be outside the United States" was not to be considered electronic surveillance, and was not to be governed by FISA, but by PAA instead (Cardy, 2008). Under the Protect America Act, the president is the one who can authorize warrantless collection of foreign intelligence information.

The president can authorize this for up to a year, under certain conditions. First, there must be acceptable procedures followed to prove the information obtained involves persons "reasonably believed to be located outside the United States." Also, it cannot be qualified as electronic surveillance, under the definition provided by the PAA. Additionally, the procurement of the foreign intelligence information involves the "assistance of communications service provider, custodian, or other person ... who has access to communications." Furthermore, a "significant purpose" must be to gather foreign intelligence information. Finally, the minimization procedures defined in FISA must be adhered to (Cardy, 2008).

As previously stated, one specific requirement necessary before the president could authorize surveillance was the assistance of communications service providers. As such, communications providers were required to aid the Attorney General and the Director of National Intelligence, and offer any technical support needed to obtain the information (Addicott and McCaul, 2008). The

act also protected these providers, including a clause granting immunity from private lawsuits to third parties assisting the government.

The Protect America Act also creates a way to review the effectiveness of itself. Within 120 days of the act's passage, FISC must review the procedures utilized, and conclude whether or not any actions should be qualified as electronic surveillance. FISC analyzes the criteria used to decide whether a procedure should be classified as electronic surveillance, using the "clearly erroneous" standard.

Finally, the Protect America Act included a sunset provision. It was scheduled to sunset six months after it was passed, on February 1, 2008. Congress extended the act for another six months, and the new version, the FISA Amendments Act, was passed in July 2008.

4.6 FISA Amendments Act

The FISA Amendments Act of 2008, better known as FAA, is an outgrowth of the Protect America Act. The Protect America Act was originally scheduled to sunset in February 2008, but was extended by another six months. Congress enacted the FISA Amendments Act before the Protect America Act expired, setting a new precedent for Internet privacy laws.

FAA was introduced into the House by Rep. Silvestre Reyes (D-TX) on June 19, 2008, and was cosponsored by Rep. Peter Hoekstra (R-MI) and Rep. Lamar Smith (R-TX). It passed by the House on June 20, 2008, with a vote of 293 to 129, and passed the Senate on July 9, 2008, with a vote of 69 to 28. President Bush signed the FISA Amendments Act into law on July 10, 2008, and it is scheduled to expire in 2012 (US House of Representatives, 2008).

FAA allows the Attorney General and the Director of National Intelligence to jointly authorize surveillance to obtain foreign intelligence information for up

to one year, given the surveillance is targeted at someone reasonably believed to be outside the United States. It goes on to explicitly forbid reverse targeting, or targeting surveillance at someone outside the United States to get information on someone located inside the United States, as well as targeting a United States person, regardless of their location (Blum, 2009).

The Attorney General and the Director of National Intelligence must still, under most circumstances, acquire a FISC order before conducting surveillance. For FISC to approve an order, three requirements must be reached. First, there must be satisfactory procedures in place to ensure it actually is reasonable to believe the suspect is located outside the United States, to prevent surveillance of entirely domestic communications. Next, the original FISA's requirements for minimization procedures must be met. Finally, both the Attorney General and the Director of National Intelligence must certify that "a 'significant purpose' of the acquisitions is to obtain 'foreign intelligence information"' (Blum, 2009). FISC then has thirty days to authorize surveillance, or provide an acceptable cause for extension.

Unlike the original FISA, there is no reference to any specific technology. With the original wording of FISA applied to the current technology, a warrant would be necessary for entirely foreign communications that were simply routed through the United States. Under the new FAA, these communications were no longer subject to FISC warrants, due to the technology-neutral wording. However, any communications involving a United States person and a foreigner are now subject to FISC warrants, regardless of the type of technology used for communication.

FAA, like the preceding PAA, requires the "assistance of an electronic communication service provider" to obtain communications (Blum, 2009). However, it allows any service provider to challenge the government's request, and appear

before FISC. The provider can appeal that decision to FISCR, and even the Supreme Court if necessary. The act also goes on to grant retroactive immunity to any telecommunications providers involved with TSP, given they present a written promise from the Bush administration that stated TSP was lawful (Blum, 2009).

Finally, the FISA Amendments Act includes several review mechanisms, to ensure there are no abuses of power. The act requires both the Attorney General and the Director of National Intelligence to create procedures to teach law enforcement how to correctly implement FAA. These procedures must be approved by both Congress and FISC before any orders can be issued. Moreover, both the Attorney General and the Director of National Intelligence must submit assessments to Congress and FISC every six months, that include "records of all proceedings before FISC, any targeting and minimization procedures implemented during the assessment period, and any incidents of noncompliance with these procedures by any element of the intelligence community" (Blum, 2009).

Finally, FAA requires that each agency executing surveillance under FAA must report every year to the Director of National Intelligence, the Attorney General, FISC and Congress. The reports should describe the use of information gleaned from surveillance, as well as how many communications involving United States persons were obtained, how many shared intelligence reports came from said communications discussing a specific United States person, how many more United States persons identities were learned and subsequently shared due to said original communications, and how many targets originally believed to be located outside the United States were later shown to be located within the United States (Blum, 2009).

5 Internet Privacy Around the World

5.1 European Union

With 500 million citizens, in 27 different countries, the European Union has faced significant challenges in dealing with policing and maintaining order on the Internet. The World Wide Web was made public in 1991, but only really caught on with the public in 1993 (Mosaic). This was the same year the European Union first formed, and the two have been growing side by side ever since.

5.1.1 EU Directive 95/46/EC

In 1995, the European Union put into effect Directive 95/46/EC, the Data Protection Act. The express goal of this act was to ensure the privacy of the members of the EU. Among the requirements were that data must be collected for explicit, legitimate purposes, and only maintained for the length of the requirement. As soon as the data was not needed, either all identifying information about the person who it was collected from must be stripped, or the data must be entirely discarded. Any inaccurate or out of date data was also to be removed immediately (European Union, 1995)

Article 7 restricted the way that the data could be gathered. By the rules set down, data could only be gathered on a person if they had given their express consent, the individual has waived their consent in a contract, or to protect the interests of the individual. There was an allowance made for data collection if it was carried out "in the public interest of an official authority...or in a third party to whom the data is disclosed." (European Union, 1995, Art. 7(e)). If any data is in fact collected, the member state must then inform the data subject who is collecting the information and why, who will be receiving the data, and

how much of the information he or she is required to supply.

Article 13 lay the groundwork for what has become common place now. Article 13 says a member state may adopt measures to waive the rights in the face of national or public security. This eventually gave way to Directive 2006/58/EC.

5.1.2 EU Directive 2002/58/EC

Having watched the United States rush to pass the USA PATRIOT Act after September 11th, 2001, the European Union wanted to ensure that their citizens were protected. Directive 2002/58/EC, the directive on privacy and electronic communications, was designed to augment and expand the 1995 directive, and focus more on the Internet. Because the Internet was relatively new when the data protection act was passed, the measures in it were not entirely appropriate or encompasing.

This directive extended the same basic protections from the data protection act to the Internet and other electronic communications. This included e-mail, cell phone calls, and any Internet traffic. Due to the unique nature of the medium though, it also offered a few new protections.

When data is sent from person to person, it rests in a network until the receiver views and accepts the data. Under Article 6, all the data must be erased as soon as it is no longer needed to be safely transmitted (European Union, 2002). Companies and service providers can only keep data longer for billing purposes or if it's important for marketing purposes, but only the information about the data can be kept, not the data itself.

The same exemptions apply from Article 13 of 95/46/EC. Retain data in the face of national security, but no methods are given as to how this should take place, leaving the decisions and the process down to the individual member

states discretion (European Union, 2002, Art. 15)

5.1.3 EU Directive 2006/24/EC — Data Retention Directive

After the train bombings in Madrid, Spain, the European Union began to focus on the largely unregulated area of the Internet. Directive 2006/24/EC, the Data Retention Directive, was proposed and passed within two months, and it overturned a lot of the provisions set forth by the 1995 and 2002 directives. While it did not go as far as the USA PATRIOT act as far as observing and monitoring it's citizens, there were significant changes.

The primary goal of this directive was to expand the capabilities of law enforcement agencies. After the 2002 directive, data on citizens could only be gathered from the point of the investigation on, as the majority of the data was deleted immediately. This meant that there was no data trail or history that law enforcement could follow about the target. This directive changed that.

Telecommunications companies were required to retain all information pertaining to the data they were transmitting for between six and twenty-four months (European Union, 2006, Art. 6). While the companies were still forbidden from keeping the actual data that was transferred, as per the 1995 directive, they were required to keep the information about the data. For e-mail, this included the senders IP address and the recipients IP address; for telephone calls or faxes, this meant the telephone numbers that were involved. The date and time of the start and end of the conversation also had to be logged. For e-mail, this meant recording the login and logout times for the users involved (European Union, 2006, Art. 3).

The member states were given until March, 2009 to enforce the directive in their territory. The only members who have not enacted it yet are Austria, Ireland, Poland, Sweden and Greece. The United Kingdom and Luxembourg

have partially implemented the directive, but have not fully enacted it yet. Romania is an interesting case, because their implementation has been declared unconstitutional (AK Vorrat, 2009).

5.2 Romania

Romania's implementation of the Data Retention Directive resulted in Law 298/2008. The data was to be held for only 6 months, which is the bare minimum time as stipulated by the Data Retention Directive. Any intentional access to the data that was held, or and non-authorized transfer of any data like this was to be punished by a minimum of one year in prison, with a maximum of five (EDRI, 2008). However, despite the leniency of the law, there was still public resistance.

In February of 2009, a group of watchdog groups sought to alert the Constitutional Court that 298/2008 limited the rights of the citizens. Their claim was dismissed however. At the same time, the Civil Society Commissariat, a Romanian civil rights group, brought a lawsuit to a major telecommunications firm regarding a promise in their contract about secure communications. Although the lawsuit itself was suspended, it was enough to bring Law 298/2008 before the Constitutional Court in October of that year. The court decided that the law did violate a core principal of the Romanian constitution, Article 28: a right to secure communications. This violation of was enough to overturn Law 298/2008 (Constantin, 2008).

There has not been a replacement law drafted yet, because of political instability in the region. The EU was notified that there would be changes, but the Constitutional Court has still not yet ruled on whether the whole law needs to be rewritten, or just the first article, which states the purpose. Whatever the court decides, it was planned to be enacted by the end of January 2010.

(Mediafax, 2009).

5.3 United Kingdom

The United Kingdom has gained a reputation in the past decade for becoming more and more watchful of its citizens. In 2005 alone, nearly 440,000 telephone wiretaps were authorized and carried out by law agencies (Thomas, 2007). While no official laws regulate the active monitoring of the Internet, there have been steps taken to oversee the safety of the citizens.

5.3.1 Anti-Terrorism, Crime and Security Act of 2001

The first act of the UK to monitor it's citizens online was the Anti-Terrorism, Crime and Security Act of 2001. In an effort to increase security after the September 11th, 2001 attacks against the United States, the UK parliament pushed this law through. One of the provisions was the ability for the government to request data to be retained (OPSI, 2001, Pt 11).

There were few regulations on what this actually pertained to, and the language was very vague and flexible. The Secretary of State was required to produce a guideline of his or her own devising on how companies should retain communications data. However, people or companies that did not comply with this the guidelines would not be attributed a criminal or civil penalty (OPSI, 2001, Pt 11(102)(1,4)). Before the guidelines could be applied though, the Secretary had to meet with the communications providers that it would affect, and once the Parliament approved it, any violation would be met with an injunction (OPSI, 2001, Pt 11(104)(4,6-8)).

5.3.2 The Data Retention (EC Directive) Regulations 2009

This is the final implementation of the EU Directive. While it is a vast improvement over the Security Act of 2001, it still does not complete every requirement of the directive. The language of the act refers in large part to telephone communications, and only mentions Internet communications in two lines(OPSI, 2009, Pt 4(1)(c),(2)(b)). The communications data that is retained is held for 12 months, and can be access by anyone with government permission (OPSI, 2009, Pt 5,7)

6 Analysis

Now that each law is fully understood, it can be effectively critiqued. The following section is devoted to analyzing all the laws previously summarized, in order to determine their successes and failures. Once the successes and failures of the past are understood, a more efficient system can be devised.

6.1 Foreign Intelligence Surveillance Act

As previously stated, the Foreign Intelligence Surveillance Act, or FISA, was the first act of its kind. As such, it was by no means perfect. It was created during a time of civil rebellion, brought on by the Vietnam War. Due to the rampant infringements on privacy rights that occurred during the Vietnam War, Congress recognized that something needed to be done to make law enforcement effective while protecting civil rights. The end result of attempting to create this balance was FISA. FISA, in theory, was a good solution to the problem at hand. It lowered the standard for electronic surveillance directed at foreign powers or agent of foreign powers, making it easier for law enforcement to gain permission for surveillance in a timely fashion. Additionally, the information required for an application regarding the suspect aimed to make certain the suspects targeted were, in fact, agents of a foreign power. Furthermore, FISA made every attempt to make sure the rights of innocent civilians were not infringed upon, by including minimization procedures in the application requirements.

The United States District Court of New York agreed with this summary of FISA, in a ruling regarding the constitutionality of FISA on its face. In The United States of America v. Thomas Falvey, Michael Flannery, George Harrison, Patrick Mullin, and Daniel Gormley, the defendants were accused of smuggling arms to the Irish Republican Army, or the IRA. The government

performed electronic surveillance on the defendants, in accordance with FISA, and had planned on introducing said surveillance at trial. The defendants then drafted a motion to suppress any information gained from the FISA surveillance, on the basis that FISA itself violated the First, Fourth, Fifth, Sixth and Ninth Amendments, as well as Articles I and III of the Constitution (United States v. Falvey, 1982).

The judge upheld the constitutionality of FISA on all counts, ruling the "FISA procedures satisfy the Fourth Amendment warrant requirement," and "FISA provisions are not over broad and unconstitutional on their face." Furthermore, the judge went on to say, in his conclusion, "I conclude that FISA is constitutional on its face." Obviously, there was no doubt about the constitutionality of FISA, at least on paper.

The way FISA was executed in practice was much different from the way it appeared in theory, however. Although the definition of what the application was evolved over time, from 1979 to 1994 the applications that came before the FISA Court were "applications made for orders and extensions of orders approving electronic surveillance under the Act" (Federation of American Scientists). In the span of these 15 years, 8115 applications came before the Court, and not a single application that came before the Court was modified or denied. In fact, a total of 8130 orders were issued, meaning the Court issued 15 more orders than requested.

While it could be argued that the law enforcement agents were simply skilled at their job, and all the applications were warranted, it seems improbable that over a span of 15 years, every single application was flawless. It is much more likely that the Court was there to rubber stamp applications, while providing an impression of judicial oversight to appease Congress and civil rights activists. Clearly, FISA was not all it appeared to be. In theory, FISA created an accept-

able system, and strong guidelines to protect against government abuses. On the other hand, in practice, it merely acquiesced to government applications, most likely facilitating the abuses it was meant to prevent.

Overall, FISA was a precedent-setting act. Despite the abuses that occurred, FISA was successful in creating a valuable model of what future legislators would look to when creating Internet privacy laws. While the execution of FISA was less than perfect, the wording of the Act and the requirements that were supposed to be met were ideal. As such, this provided a solid foundation for later legislators to create laws in accordance with the spirit of FISA.

6.2 Electronic Communications Privacy Act

The second act, the Electronic Communications Privacy Act, shortened to ECPA, was a way of applying all the previous privacy laws to the current technology. Most laws on the books applied to wire or oral communications, but with the development and increased use of the Internet, the wording of these laws were out-dated, and needed to be revamped. The first aspect of ECPA, the Wiretap Act, expanded Title III of the Omnibus Crime Control and Safe Streets Act of 1968. This section of ECPA was designed to afford electronic communications, specifically e-mails in transit, the same privacy rights given to wire and oral communications. Obviously, this was a positive step for Internet privacy. Before this act, there was no procedure in place governing surveillance of Internet communications. This act ensured the government could not conduct widespread, unwarranted surveillance on the American population.

The courts have upheld the spirit of this section of this act, in a decision made by the 1st Circuit Court of Appeals in 2005, in United States of America v. Bradford C. Councilman. In this case, Councilman was vice president of a company called Interloc, Inc., which, as a part of its service, acted as an e-mail

provider. Specifically, Councilman himself supervised the e-mail service. Councilman instructed his employees to "intercept and copy all incoming communications to subscriber dealers from Amazon.com." With this scheme, Councilman could read and copy all incoming messages before they were delivered, allegedly in violation of the Wiretap Act.

Initially, the district court dismissed the indictment, on the grounds that the "intercepted e-mail messages were in 'electronic storage' and therefore were not subject to the prohibition on 'intercepting electronic communications."' However, the circuit court overturned this ruling, stating, "We conclude that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communication" (United States v. Bradford C. Councilman, 2005). Basically, the court ruled that temporarily stored e-mails are still electronic communications, and therefore protected under the Wiretap Act.

This case shows how the judicial system interpreted the wording of the Wiretap Act; they believed the spirit of the law was meant to fully protect privacy on the Internet. This case is a perfect example of how the law did exactly what it was supposed to.

Overall, the Wiretap Act was not an especially controversial act. It merely extended the privacy rights already provided for main types of communications, to encompass a new type of communication gaining popularity: the Internet. This section of the ECPA, though not groundbreaking, was still vital. Without it, those who used e-mails to communicate would not have the same privacy rights as those who wrote letters.

The second part of ECPA was entitled the Stored Communications Act. This section was crucial, because it prevented the government from strong-arming ISPs into turning over information regarding their customers. Basically,

this section was a way of controlling how much information a third-party could share.

An example of the effectiveness of this section is the case Steve Jackson Games, Inc. v. US Secret Service, from 1993. Steve Jackson Games, or SJG, operated an electronic bulletin board system, and offered customers e-mail services, where the e-mails would be stored on the bulletin board system computer's hard disk drive until the receiver read the mail, and opted to either store it on the computer or delete it.

In 1989, the Secret Service was informed of the unauthorized circulation and copying of a computer file that provided information about the Bell Company's emergency call system. The following year, they learned the file was available on a computer bulletin board that was managed by an SJG employee. A warrant was obtained to search SJG's premises, and was executed the next day. The Secret Service seized among other items, the computer that operated the bulletin board system, which, at the time, had 162 items of private, unread e-mail. Although the Secret Service maintained they did not read any of the private e-mail, the court disagreed, saying, "The preponderance of the evidence, including common sense, establishes that the Secret Service personnel or its delegates did read all electronic communications seized and did delete certain information" (Steve Jackson Games, Inc. v. US Secret Service, 1993). The court ruled in favor of Steve Jackson Games, Inc., and awarded $1,000 in damages to each plaintiff.

This case again shows how the law was enforced the way Congress intended it to be. The court did not allow the government to overstep its authority, and read private e-mails it had no right to. This section of the act was a certainly a success, and helped to put people at ease when using the Internet, for they knew their e-mail and any information their ISP had could not be shared with

the government lightly.

The final part of ECPA is the Pen/Trap Statute. This act controls pen registers and trap and trace devices. The main reason this section of the act was included was due to a Supreme Court case in 1979, Smith v. Maryland. In this case, the Supreme Court ruled that a pen register was not a "search" as defined by the Fourth Amendment, and therefore no warrant was necessary to install one.

While the Supreme Court ruled no warrant was necessary, this section still requires some oversight, though admittedly little. However, its' explicit direction that communications content cannot be gathered ensures the act cannot be misinterpreted, or abused. In summary, this section regulated what was already allowed, and made certain powers would not be expanded. Overall, the Electronic Communications Privacy Act was successful. The act was the first to specifically include Internet and electronic communications. It increased Internet security, making people feel more comfortable online. Without this act, people would have distrusted the Internet, and it might not be what it is today.

6.3 Communications Assistance for Law Enforcement Act

The third act discussed affecting Internet privacy is the Communications Assistance for Law Enforcement Act, or CALEA. This act is important because it ensures telecommunications providers' technology is able to be surveilled by the government, and that the government can acquire call-identifying information.

As previously explained, the Federal Communications Commission, or FCC, was in charge of implementing CALEA. However, they aspired to expand the act. In United States Telecom Association v. Federal Communications Commission, the FCC attempted to force telecommunication providers to allow more information to be available to law enforcement agencies.

Overall, there were six additional capabilities the FCC was trying to force upon telecommunications providers. The four capabilities the FBI wanted to add were referred to as the "punch list." The first they requested was "post-cut-through dialed digit extraction." This basically meant the numbers dialed after the call was connected could be recorded. The second was "party hold/join/drop information," which referred to telephone numbers of parties on conference calls, and recording the times when parties joined, were put on hold, or disconnected. The third was "subject-initiated dialing and signaling information," which applied to call forwarding and call waiting. Finally, the last was "in-band and out-of-band signaling," which referenced "message-waiting indicators, special dial tones, and busy signals."

The other two were included in what was called the "J-Standard," which was a document created by the Telecommunications Industry Association to assist carriers in providing communications and call-identifying information to law enforcement. The first capability requested was antenna towers location information, as a way of locating the caller. The second capability requested was packet-mode data, which would separate the information into a non-content packet and a content packet.

The court decided in favor of the two J-Standard capabilities, agreeing with the FCC that CALEA required telecommunications providers to offer antenna tower location, and packet-mode data. However, it ruled against all four capabilities of the FBI's punch list, on the grounds that it expanded CALEA in a way that violated its original meaning.

This act was essential to Internet surveillance, because it made surveillance possible. Without this act, the telecommunications providers might not be able to separate content from non-content. This act made it possible for the telecommunications providers to separate their data, and only provide what was

necessary to the government.

6.4 PATRIOT Act

The PATRIOT Act was the next major act in Internet privacy, passed in 2001. The act was an enormous piece of legislation that was rushed through Congress as a knee-jerk reaction to the terrorist attacks of 9/11. As such, the act was not debated anywhere near as much as it should have been; to say over 1000 sections of an act can be effectively debated in two weeks is laughable. The act made drastic, and some unconstitutional, expansions to law enforcement agencies power.

Section 505, regarding NSLs, was one such expansion ruled unconstitutional, in Doe v. Ashcroft in 2004. The plaintiff, referred to as "John Doe," was an Internet access firm that received a National Security Letter under Section 505. Due to the gag order clause in the section, the Internet access firm was prevented from disclosing any information about the requests, and had to pursue the lawsuit anonymously.

The plaintiffs challenged the section on its face, and argued that the wide subpoena power violated the First, Fourth, and Fifth Amendments, and the gag order provision violated the First Amendment. The Court agreed, stating it "violates the Fourth Amendment because...it effectively bars or substantially deters any judicial process to pursue such a challenge to the propriety of an NSL request... Ready availability of judicial process to pursue such a challenge is necessary to vindicate important rights guaranteed by the Constitution or by statue... the Court also concludes that the permanent ban on disclosure... operates as an unconstitutional prior restraint on speech in violation of the First Amendment" (United States Telecom Association v. Federal Communications Commission, 2000).

Because of this ruling, the USA Patriot Improvement and Reauthorization Act, passed in 2005, made substantial changes to Section 505. First, the blanket gag order was replaced with a case-by-case determination of when a gag order is required. Additionally, the new act provided for an NSL recipient to petition a district court to modify or deny the request. If a petition is filed within one year of the NSL request, a senior FBI official merely has to certify "that disclosure may endanger the national security of the United States, or interfere with diplomatic relations," (Doe v. Ashcroft, 2004), and this was enough for the petition to be denied. This revised section was also challenged facially, in Doe v. Gonzales in 2007.

Again, the Court ruled that the gag order violated the First Amendment, and the part regarding NSLs petitions was unconstitutional, stating the standard of review set was unconstitutional. However, the court did uphold the Act's provisions to "close hearings, seal documents, and review evidence ex parte and in camera" (Doe v. Gonzales, 2007).

This section also required the FBI to submit annual reports to Congress, detailing how many NSLs were issued. In 2005, a total of 9,254 NSLs were issued relating to United States persons. In 2006 and 2007, the FBI stated that accurate NSL records were not available, but estimated 12,583 in 2006, and 16,804 in 2007, relating to United States persons. In 2008, 24,774 NSLs were requested relating to United States persons (Federation of American Scientists).

In just three years, the number of NSLs more than doubled. For two consecutive years, the FBI could not even submit accurate records. Obviously, the "judicial oversight" was merely an idea, rather than the general practice.

Clearly, this section of the PATRIOT Act failed. It was ruled unconstitutional not once, but twice. This section of the Act gave law enforcement agencies broad, unchecked power, with basically no real judicial oversight provided.

Another very controversial section of the PATRIOT Act was Section 218. The section's changing of wording from "primary purpose" to "significant purpose" has been challenged facially several times, with differing results. In 2002, In re Sealed was brought before the United States Foreign Intelligence Surveillance Court of Review. The court upheld the constitutionality of the change, stating, "Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly... that FISA as amended is constitutional because the surveillances it authorizes are reasonable" (In re: SEALED CASE, 2002).

However, in 2007, a similar facial challenge came before the District Court of Oregon, in Mayfield v. U.S., on the grounds that it violates the Fourth Amendment. The Court ruled the section unconstitutional, saying it violated the particularity of the Fourth Amendment and circumvented the normal judicial oversight required under the Fourth Amendment.

Both courts are of equal authority, and neither can overrule the other. However, the District Court of Oregon seems to have it right. The FISCR basically said in their ruling that the section was close enough to constitutional, and that is good enough. The District Court of Oregon actually analyzed what the section meant, and saw the dangers that it could bring. In its ruling, the District Court said, "The Constitution contains bedrock principles that the framers believed essential. Those principles should not be easily altered by the expediencies of the moment. Despite this, the FISCR holds that the Constitution need not control the conduct of criminal surveillance in the United States. In place of the Fourth Amendment, the people are expected to defer to the Executive Branch and its representation that it will authorize such surveillance only when

appropriate. The defendant here is asking this court to, in essence, amend the Bill of Rights, by giving it an interpretation that would deprive it of any real meaning. This court declines to do so" (Mayfield v. US, 2007).

Due to the conflicting opinions, it is less clear if this section is constitutional; an argument can be made for either side. It seems, however, the American people should never settle for "close enough" to constitutional.

The PATRIOT Act was surrounded by even more controversy in 2005, after news of President Bush's Terrorist Surveillance Program, or TSP. TSP allegedly permitted warrantless domestic surveillance by the NSA. The entire program was ruled unconstitutional in American Civil Liberties Union v. National Security Agency in 2006, with the court ruling, "TSP violates the APA; the Separation of Powers doctrine; the First and Fourth Amendments of the United States Constitution; and the statutory law" (American Civil Liberties Union v. National Security Agency, 2006).

However, it was virtually impossible for those violated by TSP to get any compensation. Several cases came before various courts, including American Civil Liberties Union v. National Security Agency in 2007, but were dismissed because the plaintiffs could not prove they were unlawfully surveilled, and therefore had no standing. Even in Al-Haramain Islamic Foundation, Inc. v. George W. Bush, where the plaintiffs, Al-Haramain Islamic Foundation, inadvertently received documentation from the government confirming their group had been monitored under TSP, the case was eventually dismissed. The document could not be admitted because it would reveal state secrets, and was a matter of national security. Initially, those who had seen the document were going to be allowed to testify to its contents, but the final ruling prevented this, saying even discussing the document would violate state secrets. As such, this case was also dismissed due to lack of standing, despite the fact everyone involved

was positive the government had illegally monitored the company.

The PATRIOT Act was such a large act, it is impossible to say it entirely succeeded or failed. Parts were successful; parts were not. However, it did exactly what it was expected to do. The American people were willing to give up their civil liberties after the attacks in exchange for increased security, and that is precisely what they got: the government ignored their privacy.

6.5 Protect America Act

The Protect America Act, or PAA, was passed in 2007, and followed the PATRIOT Act as the next major law governing Internet privacy. As shown, PAA was passed after the blatant abuse of power by the government. This act was the government's attempt to fix the problem.

Obviously, the government was unsure how to proceed, and tried something out to see if the American people would accept it and if it would make the TSP scandal disappear. This is clear because of the original short six-month sunset provision. Perhaps the government was merely trying to prevent the same abuses that occurred under the PATRIOT Act from occurring again under the Protect America Act, by reviewing it quickly to determine the effectiveness and constitutionality.

Interestingly, PAA kept the wording change from the PATRIOT Act that was facially challenged repeatedly; the changing of the "primary purpose" of surveillance is to gain foreign intelligence, to a "significant purpose" is to gain foreign intelligence. Even more troubling, the Act no longer required the target of surveillance to be a foreign power, or an agent of a foreign power. Instead, the Act simply stated the target must be "reasonably believed to be located outside the United States."

These two clauses make the Protect America Act very broad, and easily

applicable to many different situations. The wording of the Act allows for it to be applied in situations where it was not originally meant to be. Specifically, it asserted that any surveillance directed at someone reasonably believed to be located outside the United States could never be qualified as electronic surveillance, only because it was targeted at someone outside the States. This meant that law enforcement agencies would not have to get FISC approval before conducting surveillance. Then again, FISC approval meant nothing: from 1979 to 2006, 22,987 applications were made for orders. In that span, 22,981 applications were granted (Federation of American Scientists), an overall approval rate of 99.97% in 27 years. It does beg the question, however, why was it necessary to circumvent the FISC when they merely acted as a rubber stamp?

Furthermore, there was no distinction between an American citizen traveling outside the United States, and a foreigner outside the United States. Apparently, American citizens could not expect the Constitution to protect them from their own country when they were outside the border.

The Protect America Act was also challenged in the FISCR, in In re DIRECTIVES in 2008. A communications service provider directed to assist the United States in obtaining foreign intelligence information regarding a suspect reasonably believed to be outside the country challenged the legality of the Act, arguing it violated the Fourth Amendment. Though it was not a facial challenge, the Court upheld the constitutionality of the Act in this specific case, stating, "We caution that our decision does not constitute an endorsement of broad-based, indiscriminate executive power. Rather, our decision recognizes that where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts" (In re DIRECTIVES, 2008).

Overall, the Protect America Act was a very controversial act. Referred to as the "Police America Act" by its opponents (American Civil Liberties Union), it severely expanded the power of law enforcement, while restricting the privacy of American citizens across the globe. However, it was only in effect for roughly a year, before it was wisely allowed to sunset.

Replacing the Protect America Act was the FISA Amendments Act, or FAA, passed in July 2008. Currently, FAA is the most recent law governing Internet privacy, and therefore sets the precedent for law enforcement to follow.

6.6 FISA Amendments Act

The FISA Amendments Act changed some of the Protect America, and renewed others. For example, the Act kept the wording of the PAA, requiring the surveillance to be targeted at someone reasonably believed to be outside the United States as opposed to agents of foreign power. However, the Act goes on to protect those located within the United States that communicate internationally, forbidding reverse targeting. This illustrates a step towards limiting law enforcement power, and protecting the privacy rights of those within the United States.

Additionally, FAA creates more avenues for review, ensuring there will be fewer abuses of power. Instead of simply trusting law enforcement agencies' words, FAA requires every agency to report bi-annually to FISC, and, more importantly, Congress. FISC has proven its ineffectiveness already, but Congress should at least be trustworthy, and reliable to protect the privacy of Americans. These extensive review mechanisms are also a step towards the protection of the rights of Americans.

Moreover, FAA learned from the past mistakes of FISA, and kept its wording technology-neutral. The new wording makes certain those who are legitimately

suspected will not be protected due to a loophole. Furthermore, the law can be effective for a longer period, because with no specific reference to technology, it cannot become outdated easily.

FAA also requires the assistance of a communication service provider, just like the Protect America Act. However, the FISA Amendments Act allows for the providers to challenge the requests, unlike the Protect America Act. Again, another step to prevent misuse of power by law enforcement, by giving the service providers a forum to protest the orders. FAA goes on to provide retroactive immunity for providers involved with TSP. This clause was upheld in In re: National Security Agency Telecommunications Records Litigation in 2009. This case dealt with the individuals who were spied on through TSP, and were suing the communications service providers for cooperating with the government. The case was dismissed without prejudice, with the court ruling any surveillance occurring from 9/11/2001 to 1/7/2007 was to be forgiven in accordance with FAA.

However, FAA still requires a "significant" purpose of surveillance be foreign intelligence information, as opposed to the "primary." Even more, FAA does not expand the requirements for a FISC order, thereby not really improving much. The court can still be expected to be useless, because no significant changes have been made.

In sum, FAA takes positive steps towards protecting the privacy of those located within the borders of the United States. Even so, the measures taken are not drastic enough; an approval rating of 99.97% over 27 years from a court meant to prevent abuses of power is unacceptable. Changes must be made to the way the FISC operates for anything substantial to improve.

7 Conclusion

Clearly, the United States is in unfamiliar territory when it comes to combating counter-terrorism with technology. The founding fathers could not foresee the technological advances, and the complications that arose from them. Understandably, the United States law enforcement is having a rough time reconciling the constitutional rights afforded to its citizens, while protecting them from a terrorist threat.

Initially, the government struggled with this balance. What brought these laws on in the first place was the lack of balance; security dominated privacy during the Vietnam War to an unacceptable point. While FISA, in reality, did not do much, it did set a precedent for later acts. Its wording was built on over decades, slowly evolving it into something effective.

As time went on, technology expanded even more. With the creation of the Internet, and other technological advances, the previous laws were no longer applicable. People knew this, and the government feared if they did not put protections in place, the general population would not utilize the Internet, for fear of being spied on. ECPA was passed, and provided privacy for Americans on the Internet; people were not to be monitored without cause.

However, law enforcement agencies surveillance technology was not always compatible with the new technology available to the general public. If the technologies were not compatible, surveillance could not be conducted, and this was a huge problem. This brought about the passage of CALEA, which compelled any telecommunications carrier to ensure their technology was compatible with the government's surveillance technology. This guaranteed it was possible for the government to monitor suspects.

Up until then, Internet privacy laws were unobtrusive. Then, the terrorist attacks occurred. The United States has repeatedly got caught up in floods of

patriotism, and chosen to sacrifice freedoms in exchange for heightened security, and that happened again immediately after the attacks. The PATRIOT Act was passed almost instantaneously, trading American freedoms for the sake of national security. The controversial act was a response for the panic-stricken Americans, and was the government's way of assuring another attack would not happen.

Across the ocean, western Europe was also caught up in the turmoil. However, wiretapping was already commonplace, and did not need an act like the PATRIOT Act to grant the necessary permissions. Instead, the European Union took a different approach. They began to record and keep track of the comings and goings of their citizens, storing all the data, in the event that it might prove useful in the future.

However, the fear did not last forever. As time went on, the immediate threat began to fade. With the diminishing threat, the need to sacrifice privacy for protection ebbed as well, leaving only public backlash in its wake. The European Union's Data Retention Directive has come under fire for it, as well at the PATRIOT Act in the United States.

So the government tried again, with the Protect America Act. Designed to modernize FISA, it most likely was not as successful as its creators had hoped, and was allowed to sunset roughly a year after its passage. However, out of it came the FISA Amendments Act.

The most recent act is the best of its kind. The FISA Amendments Act has learned from the mistakes of its predecessors, and absorbed their successes. The review mechanisms are easily the most effective any Internet privacy act has had, and is a substantial improvement. Nonetheless, it is still lacking in certain areas, and could, without a doubt, use some improvements. So how can it be fixed? To say there is one end-all solution is oversimplifying a complicated

situation. Even so, some things could be done to improve the FISA Amendments Act while still allowing it to be effective.

More transparency would help. Wiretapping is prevalent in Europe, with the Netherlands and Italy monitoring hundreds of thousands of individuals every year. Despite the big-brother factor, however, the public does not seem to give it much thought. Even in Great Britain, where public outrage has been sparked by the closed -circuit television cameras, over 440,000 people had conversations intercepted in 2005, yet there was no outrage over that (Thomas, 2007).

The yearly reports of the FISA court consist often of three or four redacted sentences, in the name of national security. The Great Britain Interception of Communications Commissioner has to publish an annual report, that is not redacted in any way. This kind of transparency would ease the tensions of the public.

Another way to prevent abuses by law enforcement is to make them irrelevant. If surveillance was conducted in accordance with a FISC order, with a "significant purpose" of the surveillance to be gathering foreign intelligence information, foreign intelligence should be gathered. If it is not, any information gained from the surveillance should not be allowed into criminal proceedings. Denmark and Belgium both require the offense to be punishable by at least three years in a federal jail for the warrant to be issued.

This added clause would prevent law enforcement agencies, targeting those they believe to be regular criminals, from skirting the "probable cause" requirement. The FISC does not require any substantial proof that the target is involved in foreign intelligence. While this is understandable due to the secretive nature of counter terrorism, it can easily be taken advantage of. In fact, in a ruling by FISC made public in 2002, there were "errors related to misstatements and omissions of material facts" in about 75 FISA applications (Foreign

Intelligence Surveillance Court, 2002). "In virtually every instance, the government's misstatements and omissions in FISA applications and violations of the Court's orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors" (Foreign Intelligence Surveillance Court, 2002).

By requiring foreign intelligence information to be gained before allowing criminal information to be included in proceedings, it would prevent law enforcement agencies from exaggerating, and targeting regular criminals under the less-stringent terrorism requirements. It would also prevent unlawful dissemination of surveillance information. Anything shared could not be admitted in court, and any information obtained from a subsequent investigation due to said unlawful shared information would be fruit from the poisonous tree, and also would not be admitted in court.

This would prevent abuse from law enforcement agencies. However, time has shown the bigger problem is the FISA Court. With an approval rating of 99.97% over twenty-seven years, something must be done. The major change that needs to be made is the judicial standard for a FISC order. Under the FISA Amendments Act, a FISC order is to be granted, unless it is found to be "clearly erroneous." A clearly erroneous standard requires "a definite and firm conviction that a mistake has been committed" (Lectric Law Library). This means that unless the FISC judges are positive there is something wrong with the application, they must grant it. This standard is entirely too deferential, and needs to be raised.

Instead, a substantial evidence standard of review should be implemented. If this standard of review were required, "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion" would be necessary for an order to be granted (Definitions). This would mean the FISC judges

would have to support the conclusions reached by the Attorney General and the Director of National Intelligence, instead of just believing the facts of the application are true.

This may require more information to be shared with the FISA Court. However, the Court is a secret court, with its proceedings sealed from the public. As such, it is doubtful any information presented in the Court will result in a breach of national security. Furthermore, this would ensure the Attorney General and Director of National Intelligence are not exaggerating their information. With this new standard, more proof would be required, guaranteeing the orders are actually warranted. With these added changes, the laws would still be effective, while greater protecting privacy rights. These changes would make certain that the FISA orders were used correctly, and in accordance with the original spirit of the law. This is one way to strike a balance between respecting the privacy of American citizens, and successfully protecting American citizens from criminals and terrorists.

Overall, privacy and security is a very serious, and complex, issue, one that will never be fully resolved. There is no way to satisfy everyone: the left wing wants little to no government surveillance, to the point where law enforcement agencies will be ineffective, while the right wing wants over broad surveillance powers, to the point where citizens' privacy would be invaded on. However, both sides are necessary, to prevent either from becoming entirely successful. Neither side has complete control, and neither side should.

Over time, the laws governing Internet privacy have evolved to fit the society's desires; this is one trend that will never change. When a country is attacked, or in a time of war, it's citizens are in a state of panic. It is then when the majority of citizens will support the right wing, and laws will be passed to support law enforcement agencies practices of surveillance. In times of peace,

citizens are not worried about danger from an attack, and focus their attention on domestic policies. It is then when the majority of citizens will support the left wing, and demand the laws passed previously, that infringed on their privacy, be repealed or changed.

Overall, law always has been, and always will be, changing and evolving: there will never be just one solution to the problem of balancing privacy and security, but instead a large set of options. As society changes, the laws required will change as well. No final solution will ever be found to please everyone in the struggle between privacy and security. Instead, society must strive for an acceptable balance, a system where law enforcement agencies can conduct fruitful surveillance without entirely trampling on privacy rights. If this middle ground is discovered, maybe both sides will be appeased enough to agree, and this issue can finally be put to rest.

References

Addicott, Jefferey F., and Michael T. McCaul. "The Protect America Act of 2007: A Framework for Improving Intelligence Collection in the War on Terror." *Texas Review of Law & Politics* 13: (2008) 44–70.

Overview of National Data Retention Policies, 2009. http://wiki.vorratsdatenspeicherung.de/Transposition. German Data Retention Group.

ACLU Fact Sheet on the "Police America Act". Online, 2007. http://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9Cpolice-america-act.

American Civil Liberties Union v. National Security Agency. 438 F. Supp 2d 754. Dist. Court, ED Michigan, Southern Div., (2006), http://scholar.google.com/scholar_case?case=15417589282060531489&q=American+Civil+Liberties+Union+v.+National+Security+Agency&hl=en&as_sdt=40000002.

———. Court of Appeals, 6th Circuit, (2007), http://scholar.google.com/scholar_case?case=866651841477477840 2&q=American+Civil+Liberties+Union+v.+National+Security+Agency+&hl=en&as_sdt=fffffffffffe02.

Blum, Stephanie Cooper. "What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." *The Boston University Public Interest Law Journal* 18: (2009) 270–314.

Cardy, Emily A. "The Unconstitutionality of the Protect America Act of 2007." *The Boston University Public Interest Law Journal* 18: (2008) 171–196.

Christensen, Grant. "Government Information Collection: Federal Data Collection, Secure Flight, the Intelligence Reform and Terrorism Prevention Act, and the Reauthorization of the USA PATRIOT Act." *The Ohio State University I/S: A Journal of Law and Policy for the Information Society* 2: (2006) 485–520.

Romanian Data Retention Law Ruled Unconstitutional. Online, 2008. http://news.softpedia.com/news/Romanian-Data-Retention-Law-Ruled-Unconstitutional-123908.shtml.

I Definitions. Online, . http://www.ca9.uscourts.gov/datastore/uploads/guides/stand_of_review/I_Definitions.html#_Toc199130795. Section C) Clearly Erroneous.

Doe v. Ashcroft. 344 F. Supp. 2d 471. Dist. Court, SD New York, (2004), http://scholar.google.com/scholar_case?case=15299110744201350486&q=Doe+v.+Ashcroft+&hl=en&as_sdt=40000002.

Doe v. Gonzales. 500 F. Supp. 2d 379. Dist. Court, SD New York, (2007), http://scholar.google.com/scholar_case?case=7873627742897079382&q=Doe+v.+Ashcroft+&hl=en&as_sdt=40000002.

Romania Adopts Data Retention Law. Online, 2008. http://www.edri.org/edri-gram/number6.22/data-retention-adopted-romania. European Digital Rights.

Foreign Intelligence Surveillance Act. Online, 2007a. http://epic.org/privacy/terrorism/fisa/.

USA Patriot Act. Online, 2007b. http://epic.org/privacy/terrorism/usapatriot/.

European Union, The. "Directive 95/46/EC." *Official Journal of the European Union* 281: (1995) 31–50. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

———. "Directive 2002/58/EC." *Official Journal of the European Union* 201: (2002) 37–47. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

———. "Directive 2006/24/EC." *Official Journal of the European Union* 105: (2006) 54–63. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML.

Evans, Jennifer C. "Hijacking Civil Liberties: The USA PATRIOT Act of 2001." *Loyola University Chicago Law Journal* 33: (2002) 933–990.

Foreign Intelligence Surveillance Act. Online, . http://www.fas.org/irp/agency/doj/fisa/.

Foreign Intelligence Surveillance Court. "Memorandum Opinion." Online, 2002. http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/fisa_opinion.pdf.

In re DIRECTIVES. 551 F. 3d 1004. Court of Appeals, US, (2008), http://scholar.google.com/scholar_case?case=11505951744212671898&q=In+re+DIRECTIVES&hl=en&as_sdt=40000002.

In re: SEALED CASE. 310 F. 3d 717. Court of Appeals, US, (2002), http://scholar.google.com/scholar_case?case=14926646895729978023&q=%22Protect+America+Act%22&hl=en&as_sdt=40000003&as_ylo=2006.

Jonas, David S. "The Foreign Intelligence Surveillance Act Through the Lens of the 9/11 Commission Report: The Wisdom of the PATRIOT Act Amendments and the Decision of the Foreign Intelligence Surveillance Court of Review." *North Carolina Central Law Journal* 27: (2005) 95–129.

Kaas, Lisa M. "Liberty v. Safety: Internet Privacy After September 11." *Georgetown Journal of Law & Public Safety* 1: (2002) 175–89.

Clearly Erroneous Review. Online, . http://www.lectlaw.com/def/c046.htm.

Lee, Laurie Thomas. "The USA PATRIOT ACT and Telecommunications: Privacy Under Attack." *Rutgers Computer and Technology Law Journal* 3: (2003) 371–403.

Mayfield v. US. 504 F. Supp. 2d 1023. Dist. Court, D. Oregon, (2007), http://scholar.google.com/scholar_case?case=4394360232307343544&q=Mayfield+PATRIOT&hl=en&as_sdt=40000002.

Romania's Constitutional Court Rules Data Storage Law Unconstitutional. Online, 2009. http://www.mediafax.ro/english/romania-s-constitutional-court-rules-data-storage-law-unconstitutional-4972690/.

Mosaic Web Browser History. Online, 2009. http://www.livinginternet.com/w/wi_mosaic.htm.

O'Donnell, Michael J. "Reading for Terrorism: Section 215 of the USA Patriot Act and the Constitutional Right to Information Privacy." *Journal of Legislation* 31: (2004) 45–68.

ONI Home Page — OpenNet Initiative. Online, 2009. http://opennet.net/.

OPSI. "Anti-terrorism, Crime and Security Act 2001.", 2001. http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010024_en_1.

———. "The Data Retention (EC Directive) Regulations 2009.", 2009. http://www.opsi.gov.uk/si/si2009/draft/ukdsi_9780111473894_en_1.

Reporters Sans Forntieres. Online, 2009. http://www.rsf.org/-Anglais-.html.

Smith, Jeremy C. "The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security." *North Carolina Law Review* 82: (2003) 413–55.

Smith v. Maryland. 422 US 735. US Supreme Court, (1979), http://scholar.google.com/scholar_case?case=3033726127475530815&q=Smith+v+Maryland&hl=en&as_sdt=fffffffffffe02.

Steve Jackson Games, Inc. v. US Secret Service. 816 F. Supp 432. Dist. Court, WD Texas, Austin Div., (1993), http://scholar.google.com/scholar_case?case=15578406156657124091&q=Steve+Jackson+Games,+Inc.+v.+US+Secret+Service&hl=en&as_sdt=40000002.

The Wiretap Act and the ECPA. Online, 2009. http://www.unc.edu/courses/2009spring/law/357c/001/FBI/omnibus.html.

Thomas, Sir Swinton. "Report of the Interception of Communications Commissioner for 2005-2006." .

United States Telecom Association v. Federal Communications Commission. 227 F. 3d 450. Court of Appeals, Dist. of Columbia, (2000), http://scholar.google.com/scholar_case?case=12869242054085030 91&q=United+States+Telecom+Association+v.+Federal+Communications+Commission&hl=en&as_sdt=40000002.

United States v. Bradford C. Councilman. 418 F. 3d 67. Court of Appeals, 1st Circuit, (2005), http://scholar.google.com/scholar_case?case=8874715972442135816&q=United+States+of+America+v.+Bradford+C.+Councilman+&hl=en&as_sdt=40000002&as_ylo=2004.

United States v. Falvey. 540 F. Supp. 1306. Dist. Court, New York, (1982), http://scholar.google.com/scholar_case?case=11830246484640507397&q=The+United+States+of+America+v.+Thomas+Falvey,+Michael+Flannery,+George+Harrison,+Patrick+Mullin,+and+Daniel+Gormley&hl=en&as_sdt=fffffffffffe02.

US House of Representatives. *Communications Assistance for Law Enforcement Act*, 103th Cong., 2d sess., 1994. http://thomas.loc.gov/cgi-bin/bdquery/z?d103:HR04922:. To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes.

———. *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, 110th Cong., 2d sess., 2008. http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR06304:. To amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.

US Senate. *Foreign Intelligence Surveillance Act*, 95th Cong., 2d sess., 1978. http://thomas.loc.gov/cgi-bin/bdquery/z?d095:S1566:. An Act to authorize electronic surveillance to obtain foreign intelligence information.

———. *Protect America Act of 2007*, 110th Cong., 1st sess., 2007. http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.01927:. A bill to amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.