The Patriot Act: A security update for vulnerabilities

by

Lynette Hornung Kobes

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Steffen Schmidt, Major Professor
Alfred Ho
James Davis

Iowa State University

Ames, Iowa

2004

Graduate College
Iowa State University

This is to certify that the master's thesis of

Lynette Hornung Kobes

has met the requirements of Iowa State University

Signatures have been redacted for privacy

Dedication

My thesis is dedicated to my husband, Jason, my late friend, Vikki, and a very important mentor and outstanding teacher, the late Mr. Shakeshaft. It is also dedicated to my major professor, Dr. Steffen Schmidt, for his guidance and assistance with my thesis. He, too, has been an outstanding teacher and mentor.

TABLE OF CONTENTS

INTRODUCTION

The attacks of September 11th revealed some very important chips in the armor of the United States' national defense. The terrorists with these attacks also used new types of attacks, crashing airplanes into the World Trade Center and using a box cutter to overtake the pilots flying the planes. The governments of the United States and Europe recognized that some changes needed to be made. The United States passed the Patriot Act and created the Office of Homeland Security. The United States was not alone in changing its approach to new types of terrorist threats from transnational actors, such as Al Qaeda. Great Britain had legislation similar to the Patriot Act, called RIPA or Regulation of Investigatory Powers Act, which was passed in 2000. RIPA updated the laws to include new forms of technology and increased the surveillance powers of intelligence and law enforcement. France has recently made significant changes to its legal system with the Perben II legislation. French legal changes are similar to the efforts of Great Britain and the United States, in terms of making police surveillance easier to conduct. It also allows for plea bargaining. The plea bargaining change is modeled upon the process used by the United States. Democratic governments face an increased number of terrorist attacks on targets ..."yet [are] constrained by democratic principles from using many technological devices to secure those targets" (Combs, 2000). These democratic principles are at the center of the debate over the Patriot Act and the powers it grants to the government. The challenge lies in how these expanded powers interplay with civil liberties and privacy rights.

The Patriot Act was a relatively swift response to the terrorist attack by President Bush and Congress. Many critics have questioned the short time period in which this large piece of legislation was passed. The Committee on the Judiciary held one hearing on

September 24, 2001, on the Administration's proposed legislation that would become the Patriot Act. At this hearing testimony was heard from The Honorable John Ashcroft, Attorney General; Honorable Michael Chertoff, Assistant Attorney General; Honorable Larry Thompson, Deputy Attorney General; and Honorable Viet Dinh, Assistant Attorney General for Legal Policy. The Patriot Act passed in the House of Representatives with a vote of 356 in favor and 66 against. The Senate approved the Patriot Act with a vote of 98 in favor and one against. On October 2, 2001, President George W. Bush signed the Patriot Act into law.

The Patriot Act is an example of a significant piece of legislation, which attempts to provide better security to American citizens. The objective of this Act was to greatly increase the powers of the United States Government to gather, share, and act on domestic and foreign intelligence information. The Patriot Act and the centralizing unit, Homeland Security, have sought to address the problem of the different agencies, such as the Federal Bureau of Investigation, National Security Agency, Department Of Justice and Central Intelligence Agency not sharing their information with each other and thus, making the United States vulnerable in terrorist attack situations. The Patriot Act accomplishes the centralization of authority, yet retains some separate powers and divisions with various governmental agencies, who preserve and defend national security. This separation of powers and divisions helps provide the various countermeasures needed to provide security from attack. "Security is not just a matter of numerous countermeasures, but countermeasures that work independently and in series and that present different sets of challenges to the attacker" (Schneier, 2003). Individual countermeasures that are capable of working independently and in series provide another layer of protection, should one countermeasure fail. The countermeasures must be capable of working as a fail-safe measure

should an asset be compromised. Risk assessment of the assets that are a part of national security is only one aspect of security. The attacks of September 11th drove home the point that governmental agencies needed to be able to share information on potential threats to national security as a way to provide better individual countermeasures. The United States can continue the institutional separation of governmental agency duties and mission, but the information from these agencies needed to be centralized, so it can be shared and allow for stronger national security. Centralizing this information helps provide individual countermeasures to defend against an attack on any part of the system, which will work independently and/or in series.

According to Benjamin and Simon, the distinction no longer exists between: 1) foreign and domestic strategy, in terms of intelligence, law enforcement and civil liberties, or between 2) private and public boundaries, in terms of transnational terrorists attacking civilian as well as governmental targets (Benjamin and Simon, 2002). Besides blurring strategies and boundaries, additional challenges include, first, finding individual stateless terrorists, who seek to cause massive casualties, rather than enter into negotiations. This is a distinct difference from terrorist groups of the past, who were more apt to negotiate as they represented a particular nation. Second, there is a need for greater application of technological developments and information sharing about individual transnational terrorists within the United States government as well as among the United States and other nations (Benjamin and Simon, 2002).

The Patriot Act illustrates this blurring distinction of strategies and boundaries by seeking to defend on both domestic and foreign fronts in a more interconnected manner. "An integrated strategy that takes into account the military, intelligence, law enforcement,

diplomatic, and economic pieces of the puzzle will see America through" (Benjamin and Simon, 2002). The Patriot Act is a key part of this puzzle and perhaps by placing it into this context, it helps to better understand the significant role it plays in better serving national security protection.

Some measures of the Patriot Act were necessary without any question. For example, the sections which ..."decrease barriers to coordination between law enforcement and intelligence in terrorism investigations, to shore up airport security, border control and visa review procedures, and to improve controls over biochemical toxins" were needed to better defend against any future terrorist attacks (Cole and Dempsey, 2002). Other important measures include the stronger laws on money laundering and the removal of the institutional barriers, which had limited the sharing of information between intelligence and law enforcement agencies (Cole and Dempsey, 2002).

Other provisions, such as the guilty by association clause of the Patriot Act may be overly broad. For example, the Patriot Act ..."makes associational support a deportable offense, whereas the 1996 [Anti-Terrorism] Act imposed criminal penalties" (Cole and Dempsey, 2002). The American Civil Liberties Union criticized this guilt by association clause of the Patriot Act as being contrary to the civil liberties guaranteed by the United States Constitution and unnecessary because the government already possessed the right to deport an alien for just cause. "[T]he INS already had authority to detain any alien in deportation or exclusion proceedings who presented either a threat to national security or a risk of flight" (Cole and Dempsey, 2002). Thus, perhaps some governmental powers already existed prior to the Patriot Act, so some sections may be an unnecessary redundancy.

Chapter One will address how the United States is in transition with agencies being able to share information and work together in national security efforts. Chapter Two will address how we can change the data processes to make them more readily digestible and thus, make the data easier to be analyzed. Chapter Three will look at the power expansions with the Patriot Act, and explore ways the data can be collected without reducing civil liberties. If civil liberties need to be reduced, then what trade-offs are acceptable?

Changes in the actors, tools and methods of terrorist attacks are causing security challenges. Security and trust are important concepts in understanding the Patriot Act. Terrorism is another important concept, which in this context can be understood by analyzing the difference between law enforcement and intelligence. The Patriot Act is an attempt to try to improve the security measures needed by law enforcement and intelligence to provide better national security.

Security

Security is an important public good that the state provides to its citizens. A fundamental need of a nation state is the preservation and protection of that state and its citizens from outside and/or internal attack. Security fulfills the need of the nation-state to have a strong military, weapons and countless security measures, such as spy satellites and other technology to detect potential attacks. "Security is, after all, the most basic of basic human needs" (Strange, 1988). The state provides the security to guard against threats from other nations, transnational actors, such as terrorist groups, or from an internal threat posed by a disgruntled or mentally insane citizen. The Patriot Act addresses these basic needs of the state to provide security for the nation and its citizens. The purpose of the Patriot Act was to improve the investigative tools and information sharing for law enforcement and

intelligence agencies in their quest to protect the United States from terrorism and terrorist related activities (Patriot Act, 2001). The Patriot Act specifically states that "[t]o protect the delicate balance between law enforcement and civil liberties, the bill provides additional government reporting requirements, disciplinary actions for abuse, and civil penalties" (Patriot Act, 2001). Therefore, the Patriot Act recognizes the balance in democratic government between the needs of law enforcement, such as surveillance, and the guarantee of various civil liberties, such as the guarantee of the Fourth Amendment to be free from unreasonable search and seizure. Security has various costs, including the checks on governmental power, to prevent it from trampling upon civil liberties as well as economic costs.

Costs of Providing Security

The state incurs substantial economic costs to provide security, in terms of the money needed to conduct research and development of technological tools to combat terrorism as well as providing a strong military and weapons to fight an attack. The citizens of a nation also pay a price for their security. Their tax dollars support the government in providing the military, weapons and research to provide new forms of protection. Citizens also pay for the cost of security by granting the state access to various databases and information, which some claim infringe upon personal civil liberties and privacy. Susan Strange refers to this cost as the loss of free choice (Strange, 1988). Databases that contain personal information on citizens spending habits, contact information and other records of personal habits may be necessary to assist law enforcement in tracking criminals, but it also is a loss of privacy for average citizens. The great debate between supporters and opponents of the Patriot Act

revolves around whether this act provides security in an appropriate manner or provides security by sacrificing civil liberties.

Law enforcement and intelligence need time to gather evidence. This time has a cost, in terms of the technological tools that are needed to conduct the search as well as the salaries of the officers involved and other overhead costs. Another significant cost is the due process procedure. Due process was designed to ensure that evidence was obtained by legal and ethical means by making it somewhat cumbersome for the police and intelligence services to tap into the privacy of people. These protections, however, came under scrutiny, especially by the Bush administration, law enforcement and intelligence agencies, after September 11th because they were seen by some as having made it difficult for law enforcement to gather and put together pieces of evidence to uncover the terrorist plot and/or arrest the terrorists before they could carry it out. On the other hand, critics of new, more intrusive, and harsher measures, such as the Patriot Act have argued that the existing laws were more than sufficient to have stopped the attacks. They argue that it was bureaucratic infighting, poor police work, under-funded agencies, and incompetence that led to the intelligence failure. Better management, competent communication and teamwork are the solutions to this failure of management, not the new harsher laws. The harsher laws are not only unnecessary, but are a threat to American civil liberties traditions.

A fundamental need of a nation state is the preservation and protection of that state and its citizens from outside and/or internal attack. In the current era of military defense, the rules of engagement have been modified to include more advanced technological forms of weaponry. Just as Mercantilists approach politics and the economy by having the state drive the economy, so the state has also supported its domestic producers of goods and services.

The Patriot Act seeks to strengthen this partnership between the government and private industry because private industry provides the technology that government and private citizens use to conduct their business. For example, law enforcement and intelligence have to work with Internet service providers to obtain electronic information about communications made by suspected terrorists. Technology provides many tools used for security purposes.

Technology and Security

Although technology provides many significant tools to provide security, it is not the only tool needed. "They [law enforcement, civic leaders and engineers] believe that because technology can solve a multitude of problems and improve our lives in countless ways, it can solve security problems in a similar manner" (Schneier, 2003). Security does not simply involve the prevention of attacks by various attackers nor does it only consist of technological solutions to problems. It involves providing many measures and countermeasures, some involving technology and others involving the use of human actors, to provide multiple layers of security. Law enforcement and intelligence officers are trained to detect various human behaviors that indicate criminal or terrorist behavior. Thus, technology greatly assists law enforcement and intelligence in their efforts to provide national security, but it also involves noting human patterns of behavior.

One example of the use of technology to aid with security is the computer system, CAPPS. CAPPS is the Computer-Assisted Passenger Profiling System, which the Federal Aviation Administration or FAA has been using since 1999, ..."to identify high-risk individuals for increased security attention" (Schneier, 2003). The version that is currently used is CAPPS II. Security is difficult to ensure even with a strong system, so if a terrorist

falls into the category which does not get regularly tagged as belonging to suspect category, then he or she may be able to bypass the system. Also, even good databases are not enough in democratic nations as due process is an appropriate check upon the use of data bases. The constraints upon security are time, cost and infrastructure. CAPPS does appear to be effective as it is used in conjunction with random searches in the airports (Schneier, 2003). However, the technology alone is not enough to provide adequate airport security. It is the use of technology with the human component of random searches, which makes this approach to airport security effective.

Before security measures and countermeasures can be employed, potential attacks and/or threats must be identified, authenticated, and appropriate governmental response must be authorized (Schneier, 2003). The government needs appropriate technological tools to identify, authenticate, and authorize the legal response to a potential or actual breach of security. Technological tools are not enough, there also needs to be human involvement in providing security. Governmental agencies must train, practice and test a developed set of instructional procedures to respond to an emergency attack on critical infrastructures, such as CERT (Critical Emergency Response Team). Critical infrastructures include various aspects of basic economic and human consumption needs, which citizens need for basic survival. In 1998, President Clinton issued the Presidential Decision Directive 63 or PDD 63, which identified eight different critical infrastructures that the government and private sector were charged with joining forces together to protect from attack. These eight critical infrastructures were identified as "(1) information and communications; (2) banking and finance; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of

government; (7) electric power, oil and gas production and storage; and (8) public health services" (Dacey, 2002). An attack on any one of these structures would not only affect American citizens' daily social lives, but also our economy, as well as our military and government.

Security System Analysis

In analyzing security to combat terrorism, it can be approached with a series of four steps: 1) identify the assets that need protection, 2) identify the risks that threaten the assets, 3) analyze how effective the security solution is at minimizing the risks, and 4) identify other risks, such as long-term ones (Schneier, 2003). Terrorists may select anything with regard to assets, especially the non-obvious target, like the World Trade Center. They may also target governmental buildings, such as the Pentagon. However, the transnational terrorists of today use novel methods and targets. Security typically screened for bombs, guns and knives, but box cutters are a more novel method of attack. The risks are any type of information which can be used to launch an attack. Again, the non-obvious can be a risk, such as being granted a visa to enter a nation and be trained at that nation's flight school. The security solution must be constantly revisited as new tools and strategies are employed by terrorists. This is what the Patriot Act attempts to achieve. States have an ongoing challenge to update the laws on different tactics employed, such as money laundering on a vast network and other strategies that we do not have the opportunity to identify until after the fact. It is a challenge to identify short term and long term strategies, but this is the only solid approach to best serve any nation combating terrorism. Vulnerabilities are not easy to detect in a ubiquitous manner and because terrorists need to be secretive to be able to attack their targets, it is even more difficult.

Terrorism

Security tries to protect against and/or mitigate attacks. One of the primary types of attacks that security tries to protect against is terrorism. "Terrorism is an act comprised of at least four crucial elements: (1) It is an act of violence, (2) it has a political motive or goal, (3) it is perpetuated against innocent persons, and (4) it is staged to be played before an audience whose reaction of fear and terror is the desired result" (Combs, 2000). Contemporary terrorist are more apt to target the civilian population as opposed to governmental officials and/or targets, which were the targets of more traditional terrorist groups. The United States has struggled with how to better enable intelligence and law enforcement to protect against terrorism. A major challenge with creating legislation to better protect against terrorism is how to keep terrorism policy in line with the Constitution. As the Anti-Terrorism Act of 1996 and the Patriot Act illustrate, when we have terrorism policy, which skirts the Constitution, it is not effective (Cole and Dempsey, 2002). Both legislative acts attempted to strengthen the ability of intelligence and law enforcement to pursue and prevent terrorists from attacking the United States. The United States has a history of keeping foreign intelligence somewhat separate from the domestic police powers of law enforcement. The Patriot Act, in its efforts to increase the sharing of information between and among federal agencies, has made this separation less distinct.

CHAPTER ONE: INTELLIGENCE AND LAW ENFORCEMENT

The Central Intelligence Agency or CIA was established in 1947 to conduct foreign intelligence only. The CIA was intentionally not given domestic police powers or the power to subpoena as it was designed to provide secretly gathered information to the President of the United States to assist him or her in carrying out national defense and foreign affairs (Cole and Dempsey, 2002). However, with the attacks of September 11th, the Patriot Act sought to increase the sharing of information between governmental agencies, including between intelligence and law enforcement agencies. The Patriot Act allows law enforcement to share grand jury investigation proceedings, wiretaps and other information, which constitutes "foreign intelligence" with the CIA (Cole and Dempsey, 2002). Yet, the sharing of grand jury information (confidential) with intelligence agencies, which are not part of the domestic criminal justice process, contradicts the separation of foreign intelligence from domestic police powers.

The late Supreme Court Justice, Louis Brandeis, stated that the Framers of the United States Constitution understood ..."that fear breeds repression; that repression breeds hate; and that hate menaces stable government" (Cole and Dempsey, 2002). It is for this reason that the elaborate system of checks and balances were created to check the governmental branches with each other. It is also the reason that various civil liberty and Constitutional protections were afforded to those accused as a check upon the government's power with regard to individual citizens. "In the U.S. and many other countries, citizens have deliberately put in place all sorts of laws that hamper or constrain the police—for example, limits on lawful interrogation, search and seizure rules, and rules for gathering evidence" (Schneier, 2003). Historically, the state frequently abused its exercise of power as it applied

to the arrest and prosecution of citizens accused of specific crimes. These experiences led citizens to convince their legislators to pass laws, which provided various Constitutional and legal guarantees regarding the arrest and prosecution of those accused of a crime. One example of a check upon the government's power over citizens is the Fourth Amendment. The Fourth Amendment established the right of citizens to be secure against unreasonable search and seizure in their "persons, houses, papers, and effects" (Rosen, 2000). Another check upon law enforcement is the grand jury.

Law enforcement, unlike foreign intelligence, must adhere to checks and balances, such as the grand jury. The grand jury was originally designed to prevent the prosecution from abusing the criminal justice system in pursuing defendants, who committed criminal acts (Cole and Dempsey, 2002). The grand jury process has evolved to one that allows for investigation, in terms of being able to compel testimony from witnesses who the prosecution calls for, and being able to charge witnesses with perjury, if they lie on the stand.

There are two significant checks upon the power the government can exercise in the grand jury process. First, the government must meet due process requirements on any evidence or testimony used from the grand jury proceedings. These requirements are that the government must prove beyond a reasonable doubt that the defendant is guilty and that the person accused has a right to confront his or her accusers (Cole and Dempsey, 2002). Should it be found that any testimony is inaccurate or misleading then the innocent person does not suffer any egregious harm as this testimony is thrown out and charges may be dismissed. Second, any evidence or testimony, which was not used in open court proceedings, can only be used for law enforcement purposes and must be otherwise held in confidence (Cole and

Dempsy, 2002). Thus, witnesses who provide important testimony will be provided with protection as they are material witnesses to the prosecution of the defendant.

Law enforcement is restrained by the various Constitutional requirements, which provide protection for the accused, as law enforcement carries out its duties of bringing to justice guilty individuals. Thus, it is a very different climate than that of intelligence, which operates more covertly in its information gathering. The evidence intelligence collects on suspected terrorists or other enemies of the state, is not typically introduced as evidence in a court of law. Section 203 of the Patriot Act amends Rule 6 (e) of the Federal Rules of Civil Procedure, "to allow information collected by grand juries to be shared with the CIA and other intelligence agencies, as well as any national defense or national security official, without the prior approval of a judge" (Cole and Dempsey, 2002). This translated into the CIA being able to work with law enforcement in issuing subpoenas, which violates the limit on intelligence not being able to exercise the various powers, which law enforcement possesses within the constraints of due process. Furthermore, there are no limits placed upon this sharing between law enforcement and intelligence, which to be Constitutional, should include judicial approval to share grand jury proceedings and other investigative powers exercised by law enforcement with intelligence (Cole and Dempsey, 2002). The United States is not the only democratic nation to struggle with the roles of intelligence and law enforcement in providing security. Great Britain and France have struggled with these same issues of providing national security in a new era of terrorism.

Security in Great Britain and France

The United States has a security tradition of not distinguishing between law enforcement and intelligence. Indeed, the Patriot Act attempts to strengthen various forms of

governmental surveillance that focuses largely on security measures needed to protect our nation from terrorists. From our nation's inception, there has been a strong tradition of seeking to provide security to the United States and its citizens, while maintaining certain privacy rights that are guaranteed in the United States Constitution. Sometimes to gain a deeper understanding of how significant legislation, like the Patriot Act, fits into the broader scope of what other nations do to address terrorism and law enforcement needs, it is useful to do a comparison. This helps to place the Patriot Act within the context of what other democracies do to combat terrorism with their intelligence efforts and how civil liberties and privacy with their own citizens are handled within this context of national security. France and Great Britain have a slightly different approach to providing national security and weighing in on privacy and civil liberties in their nations. France and Great Britain can exercise greater latitude in regards to opening citizen mail and conducting phone taps. They also have different history with regard to the relationship between government and intelligence as well as the structure of their intelligence.

Great Britain and France are an interesting contrast to the United States, in terms of surveillance that they conduct for security purposes. France has a long history, dating back to the French Revolution of 1789 and Napoleon of opening letters on the domestic front. This was done initially by the "cabinet noir". This cabinet noir were postal spies that served the French state and had the purpose of preserving France (Porch, 1995). The Revolution of 1848 eliminated the cabinet noir, but the French government has retained its broad latitude to monitor the mail of its citizens domestically.

France

There are two reasons that domestic, not foreign surveillance in France has been so thoroughly developed into a bureaucracy. "The first is that, in France, domestic surveillance was the foundation stone of foreign intelligence" (Porch, 1995). France's history of granting political asylum to foreigners, who were often revolutionaries, necessitated that there be strong domestic surveillance. France, as opposed to the United States and Great Britain, has always found it very difficult to distinguish among domestic surveillance, intelligence, and foreign intelligence (Porch, 1995). The consequence of such fragmentation has been a lack of clear direction and leadership from the French government and within intelligence as well. While some may claim that there is strength that comes from having information gathered from multiple sources of intelligence, this has not been the case with France. Information gathered from multiple sources has not been centralized in such as manner that meaningful analysis and interpretation of this information can be accomplished. Such meaningful analysis and interpretation is one of the goals of the Patriot Act and RIPA. Perhaps France needs to create legislation which seeks to accomplish this goal as well.

The second reason was that there was no international threat to the French army until 1866 (Porch, 1995). By 1866, French military intelligence had deteriorated and the focus on domestic, not foreign, surveillance provided no incentive for France to have well-developed cryptanalytic skills. Part of the reason for the deterioration of the French military intelligence was the weak governance under Louis Napoleon in the Third Republic. Specifically, the Third Republic had a series of governmental experiments ranging from monarchies to republican forms of government. These governmental experiments failed to provide the strong leadership necessary to centralize the various intelligence agencies.

Instead, the Third Republic ..."encouraged the natural tendency of the ministries of the Interior, War, and Foreign Affairs to gather intelligence in isolation" (Porch, 1995). Such lack of communication from within intelligence agencies also happened to the United States with the September 11th attack and the Patriot Act has sought to address this communication problem.

The Fifth Republic did not succeed much better than the Third as French intelligence was not held accountable and suffered from various scandals and failures between 1958 and 1981 (Porch, 1995). Thus, French intelligence was too busy trying to deal with its failures and scandals and, as a result, did not have adequate time to actually conduct thorough intelligence gathering and analysis. These same problems also plagued the Fourth Republic, which perhaps in some ways set the stage for the Fifth Republic. The lack of a strategic policy and strong alliance between the French President and the French intelligence, coupled with weak foreign intelligence, translated into a situation where French intelligence suffered from a lack of support and direction from the President. Perhaps French intelligence was spread too thin in its various interactions with French colonies, like the French Indochinese War. Its own domestic intelligence tried to do too much with a small number of resources and ineffective leadership from within as well as a lack of political direction from the government.

President Charles de Gaulle's leadership approach was to have French intelligence immediately implement his policy commands (Porch, 1995). The problem was that French intelligence was unable to move as quickly as he wanted. Another complication with de Gaulle was that he trusted his diplomats, not French intelligence. In fact, the French secret services were dependent upon the CIA (Central Intelligence Agency) for foreign intelligence,

which de Gaulle ordered the severance of after 1963 (Porch, 1995). The factor influencing de Gaulle's break from the CIA was that the CIA had information that there were Soviet spies in the SDECE (Service de Documentation Extérieure et de Contre-espionage), which President Kennedy communicated in a letter to de Gaulle. President de Gaulle interpreted this as a lack of confidence by the United States in the Fifth Republic and a disagreement over French policy (Porch, 1995). He believed that his ideas on French policy were different than what the United States saw as French policy. In de Gaulle's mind, the United States exerted far too great an influence on France, which is why he sought to separate France from the United States on various political levels, such as severing ties with the CIA.

Perhaps some of de Gaulle's paranoia about a lack of confidence in French intelligence was well-founded. For example, the British MI5 did not have very much confidence in the reliability and strength of the French intelligence because they felt there was too much Soviet influence on the Free French movement. "First, intelligence was increasingly pressed into the service of domestic surveillance. Second, de Gaulle tolerated the creation of parallel intelligence networks, with informal links to the regular service, to carry out policies he preferred not to entrust to his regular services. Both practices proved to be dismal legacies to the secret services of the Fifth Republic" (Porch, 1995). The creation of parallel intelligence networks further fragmented the French intelligence efforts and reduced its effectiveness and efficiency.

In terms of domestic surveillance, the Renseignements Généraux or RG had collected huge files on French citizens who were in trade unions and political groups by conducting telephone wiretapping, opening mail, and gathering opinions. In fact, ..."domestic spying is so embedded in French political culture that politicians, police, and even judges rarely saw a

telephone tap they did not like" (Porch, 1995). There are three types of telephone taps: 1) administrative, 2) judicial, and 3) unauthorized. Administrative phone taps are requested by the Prefecture of Police, the Ministry of Defense, or the Ministry of the Interior and must be approved by the Prime Minister's office before they are forwarded to the GIC's (Groupement Interministériel de Contrôle) phone tapping center (Porch, 1995). The judicial phone tap, which is granted by a magistrate to the police, is the most subject to abuse (Porch, 1995). Once a magistrate grants a judicial phone tap, the tap is conducted by a private firm. Former police officers frequently work at such private firms and are the parties responsible for administering the phone tap. The third and unofficial type of wiretap is the unauthorized or "sauvage" phone tap. For example, a tap may be carried out as a favor to a former colleague without going through the appropriate channels to obtain a judicial order (Porch, 1995).

Unlike the American judicial system, transcripts of phone taps are not admissible in French courts (Porch, 1995). However, because the French population understands that domestic wiretapping is done fairly regularly, they tend to talk in code or otherwise self-censor their conversations. Thus, widespread wiretapping is conducted regularly on French citizens by their intelligence agencies, but this information is not used in court proceedings. The Patriot Act expands the length of time that law enforcement can conduct surveillance, whether it is phone or electronic communication. This evidence, provided that it was legally obtained from such surveillance, is admissible in court. The subsequent question is which approach better safeguards the civil liberty and privacy rights of individuals? Is it better to have your communication regularly monitored, but not used as evidence in prosecution, or better to have communication monitored only when certain criteria is followed (due process) that can be used as evidence in the prosecution? Perhaps at this point judgment should be

reserved on answering these questions until there has been more time to analyze how law enforcement has been using their expanded powers of the Patriot Act and to note if France creates any changes to their system that would start to make wiretapped conversations admissible in court.

France suffers from intelligence agencies that engage in turf wars, so there is a lack of communication between the various intelligence agencies as well as a governmental policy of trying to negotiate deals with terrorists. The various French intelligence agencies, instead of working together in a supportive alliance, compete against each other and are rather distrustful of each other. A further complication is that the French government has a history of cutting deals with terrorists in exchange for immunity from terrorist attacks. However, this is not always a good exchange as France does not always receive insulation from terrorist attack. For example, there was a bomb attack on Orly airport in Paris by Arab terrorists groups, that was done in retaliation against France for what the terrorists deemed "pro-Zionist policies" in Lebanon and the Iran-Iraq War (Porch, 1995). Thus, French intelligence agencies do not communicate and work well together and the French government tries to negotiate independent deals with terrorist groups. This lack of internal teamwork and lack of governmental support have undermined their efforts to protect France effectively from terrorist attack.

The French intelligence culture contributes to the difficulty of intelligence and the government being able to protect France from terrorism. "Rather than rationalize and modernize the relationship between French intelligence services and the state, the Fifth Republic has accentuated some of the worst features of French intelligence culture: the intermixing of domestic or counter-intelligence with foreign intelligence continues because

the frontiers between internal and external enemies have not been easy to define" (Porch, 1995). All nations struggle with the challenge of internal legal restrictions, such as due process, which inhibit the ability of law enforcement and/or domestic intelligence to try to keep track of internal enemies. Likewise, foreign intelligence has the continual challenge of trying to protect against external enemies. This has contributed to the fragmentation within the French government and intelligence, which makes France vulnerable to international terrorist attack.

Fortunately, the United States has not suffered from France's cultural problem of not drawing a distinct line between domestic and foreign intelligence. The United States' tradition has been one of having broader latitude for intelligence to gather information on foreign intelligence, but employing a narrower standard to domestic intelligence because of the cultural tradition of limited government and protection of civil liberties based upon Constitutional guarantees. Constitutional guarantees, such as the Fourth Amendment's protection against "unreasonable search and seizure" applies to a person and their home and possessions.

Great Britain

British secret services have been around since the Restoration and Vote of 1797. The Joint Intelligence Committee or JIC is similar to the CIA of the United States. The JIC gathers information on foreign threats to British economic, political, or military interests (Herman, 2001). Similarly, the CIA gathers information on ..."foreign, defense and economic policy, and the protection of United States national security interests from foreign security threats" (Herman, 2001). Securing national security is more complex with the increased ease of global communication via the Internet and travel. Thus, the new threats to

security are not so much other nations as it is transnational actors, like Al-Qaeda and other radical groups. These new threats to security may derive from ..."economic espionage and the covert collection of scientific, technical and financial secrets have had worldwide publicity as growth areas" ...(Herman, 2001). This technical, scientific and financial information could be used to plot various types of terrorists threats and are difficult to guard against because there will always be a black market for such information. Perhaps nations could ally themselves to share any information on any covert collection and future sale with the nation or nations affected, but this is problematic as it would probably require data collection on a vast array of citizens and thus, violation the right to privacy. Another solution would be to make information open source, which is of use to intelligence.

"In the world of secret services, Open Source Intelligence (OS-INT) means useful information gleaned from public sources, such as scientific articles, newspapers, phone books and price lists" (Stalder and Hirsh, 2002). The concern with open source intelligence is that there will be extensive data mining of individual citizens, which will violate various civil liberties and the right to privacy. An additional concern is that any data that is mined for security purposes would be done in a manner that is somewhat separate from due process procedures (Herman, 2001). These concerns are of primary importance in the United States and Great Britain and more recently is of greater concern in France. The increased surveillance power granted to the French police has created concern over data mining and the loss of privacy with French lawyers and citizens. However, because security intelligence collects covert information, it must be able to secretly gather information on its targets without being unduly constrained (Herman, 2001). There is a fine line that intelligence must walk to adequately perform its duty of providing national security, but in doing so, must not

unduly infringe upon individual civil liberties and privacy rights, which is the concern of those that oppose the Patriot Act.

Great Britain and the United States as Intelligence Models

The British JIC is an interdepartmental system, whereas the American CIA is a centralized agency. Both the JIC and the CIA have served as intelligence models for other Western nations, including the European Union (Herman, 2001). However, a fundamental difference that the United States possesses, which is one central issue with the Patriot Act, is that it does not distinguish between typical law enforcement and security intelligence (Herman, 2001).

Both the United States and Great Britain adhere to the two faceted aspects of intelligence, which are single source and all source information (Herman, 2001). Single source information comes from the covert information that intelligence collects. The British SIS or Secret Intelligence Service gathers foreign intelligence from human and technical sources in a single source collection manner. By contrast, the JIC and DIS (Defense Intelligence Staff) gathers and analyzes security information in an all source manner (Herman, 2001). All source information is the more comprehensive intelligence information that intelligence agencies gather for the government to help it maintain national security. Both single source and all source information assists British and American intelligence in providing information to be used to prevent an attack and possibly assist in the capture of known or potential terrorists. Although Great Britain and the United States use the two types of information for intelligence, they do have slightly different approaches to solving intelligence problems.

Great Britain and the United States have different approaches to intelligence, in terms of the paradigm in which they view the problems that intelligence seeks to solve. "The British are inclined to view American intelligence as the product of an engineering culture, always trying new solutions for insoluble problems, and ignore what this US restlessness achieves" (Herman, 2001). The engineering approach has in many instances served American intelligence well. For example, United States satellite technology has been effective with the surveillance that it has engaged in. Furthermore, United States financial investment for intelligence collection, surveillance and reconnaissance (ISR) is substantial as it surpasses ..."that of all other nations combined" (Herman, 2001). Great Britain, by contrast, is not as inclined to embrace technological developments to assist intelligence. Instead, they prefer to work in a more systematic and incremental fashion. Maybe it is this lack of sophisticated technology by the British, which has not created the same threat to individual privacy that technology has created in the United States. However, because there is a fear of technological attack with any industrialized nation, perhaps more nations will look to the United States as to how it is working to secure critical infrastructures from attack. As nations explore how to better defend themselves from the new non-obvious threats of terrorism, they may also revisit how centralized their intelligence should be.

The United States is far more centralized in its intelligence structure than either Great Britain or France. Intelligence in the United States is distributed among agencies and in different physical locations, such as the CIA at Langley, Virginia, and NSA at Fort Meade, Maryland. By contrast, in Great Britain the intelligence agencies are more condensed and in closer physical proximity, with the exception of Sigint and the imagery centers (Herman, 2001). Sigint stands for signals intelligence. The Government Communications Headquaters

(GCHQ) uses Sigint to monitor communication, including electronic and other forms of communication (Herman, 2001). It is this centralization that also creates concerns over data mining of private information on individual citizens.

Conclusion of the French and British Comparison

France has a history of strong domestic surveillance and widespread use of wiretaps. However, its intelligence agencies have suffered from internal competition and a lack of strong political leadership over the last three republics. The political leadership has not trusted the French intelligence as much as its own diplomats, which has led to strong fragmentation and a lack of central policy to help it be effective. Perhaps France needs to draw actual distinctions between its domestic intelligence, intelligence and foreign intelligence to help law enforcement be more effective at what it does with surveillance. Better cooperation between the President and French intelligence would also be a step in the right direction. France may have their chance to work on this with its recent legislation, Perben II.

Great Britain is less centralized than the United States with its intelligence, in terms of structure and the exercise of power. However, there is the common thread of British intelligence agents being educated together because those that seek government jobs are educated at the same school. This culture of education shapes the philosophical approach that British intelligence takes towards approaching the protection of national security, which serves as a centralizing agent. By contrast, the United States is more apt to look to new engineering solutions to help solve various intelligence problems, which is a different approach than Great Britain takes. However, there are some significant similarities as well. Both engage in single source and all source information. Citizens in both nations have civil

liberty and privacy concerns with the data mining that is done with open source intelligence information gathering.

France, Great Britain, and the United States all break their intelligence into an agency that deal primarily with internal security and an agency that deals with national security from external threat. Thus, the DGSE (Direction Generale de la Securite Exterieure), ..."like the CIA or MI6, aimed to gather intelligence on foreign threats to France, while the DST, like the FBI or MI5, is responsible for interior security" (Porch, 1995). The interesting differences lie in how France, Great Britain and the United States conduct their surveillance, in terms of balancing security and privacy. Security and privacy are very much central to the Patriot Act and serve as a dividing line between supporters and critics of the Patriot Act. Supporters of the Patriot Act believe that national security should be of primary importance, whereas critics of the Patriot Act believe that privacy rights should not be sacrificed in the quest to provide national security.

Great Britain and France do appear to be exploring whether they need to enhance the power of their governments to conduct surveillance to provide better national security. Great Britain and France have both created new legislation, similar to the Patriot Act, to expand the power of the government to use more current technology to intercept communication by criminals and increase surveillance abilities. Great Britain enacted RIPA in 2000. Like the Patriot Act, RIPA has updated the law to grant the government the power to intercept communication used in electronic communication. "It also puts other intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act" (The Regulation of Investigatory

Powers Act, 2000). France has made legal changes with the passage of Perben II, which have expanded the power of the government as well. Perben II is named after the French Minister for Justice, Domenica Perben. Perben II makes several revisions to the French penal code, including the change of the waiting period for suspects who can be detained and questioned without being formally charged from two to four days (Sciolino, 2004). Perben II also grants police the power to pay informers, enter into suspects' dwellings and install hidden microphones and cameras to gather information on alleged criminal activity and the power to penetrate criminal gangs (Henley, 2004). Perben II makes the unprecedented change to the French legal system of introducing the plea bargaining process, based upon the United States' model. French attorneys have responded to these significant changes to the legal system by protesting and going on strike. They claim that these new powers granted to the government will result in abuses of power by the police and that French citizens are losing their privacy.

As public policy concerns of how security surveillance is exercised with regard to individual privacy and civil liberties is evaluated, the question becomes does the Patriot Act need to better distinguish between the increased security measures it provides to combat terrorism from non-terrorist law enforcement activities? Such a change in approach would be a sharp break with the traditional approach which is unique to the United States of not drawing this boundary line. Great Britain and France, by contrast, have had a more cut and dry line regarding security and privacy, with a broader latitude granted to their intelligence to conduct surveillance. However, such surveillance is not admissible in French court and since September 11, both France and Great Britain have been tightening up their anti-terrorism

laws as well. Perhaps, they, like the United States will have a debate similar to that of the Patriot Act, in terms of security versus privacy.

One solution to the concern that surveillance powers granted by the Patriot Act are a threat to privacy rights is to overhaul our domestic intelligence. Some former CIA, FBI and Pentagon officials have suggested that the United States needs to create a domestic intelligence service housed in the FBI and managed by the Director of the CIA (Risen, 2003). However, such a radical cultural and organizational change would require a lot of forethought and planning before implementation. As illustrated by the French model of intelligence and the United States with the lack of communication between agencies prior to the September 11th attacks, different governmental agencies are territorial, possess their own distinct culture and often compete against each other. Thus, such a jointly governed domestic intelligence entity would require serious culture change. Such a change would require strategic choice and direction determined in excruciating detail before implementation. Maybe the problem is not as much a need for an overhaul of domestic intelligence, but instead, is the need for better analysis of the data and information collected.

CHAPTER TWO: DATA COLLECTION AND TRUST

Security only works if there is trust. Databases, computers, networks and the individuals charged with overseeing these technological entities must all be trusted. There are several checks upon such systems and people that must be employed to guarantee trust as best can be done. Nothing is fool-proof. A three prong approach of prevention, detection and response work together to create a network of trust for individuals (Schneier, 2003). Detection and response are very important as it will never be easy to prevent all terrorist attacks. However, being able to collect and analyze the data and use that information to minimize the impact of an attack or attacks is central to any strong national security.

Data is easy to collect, correlate, use and abuse (Schneier, 2003). It is easy to search for computerized data. "Networked data can be searched remotely and then collated, cross-referenced, and correlated with other databases" (Schneier, 2003). Data that is collected and stored makes it vulnerable to various types of attacks on the network, etc. It is important to compartmentalize the data, in terms of breaking the data assets into smaller pieces to secure each one separately (Schneier, 2003). Dynamic security is safer than static security. Dynamic security is constantly assessing and re-assessing the countermeasures and how the countermeasures respond to an attack. Static security has demonstrated through-out history that if a security system is developed and not continually updated against new forms of attack, then it will eventually be attacked by a new form and will fail.

Data Versus Information

There is a difference between data and information (Schneier, 2003). Data is like a footprint of what the information can mean. The investigation into the September 11th attacks are revealing that the NSA, FBI, and CIA all had data indicating that an attack would

occur, but it was not analyzed in time to prevent the attack. In all fairness, there is no way that intelligence agencies can always analyze all data, leads and tips, but that does not mean that intelligence should not attempt to improve its detection, prevention and response abilities. "The problem isn't *obtaining* data, it's deciding which data is worth analyzing and then interpreting it" (Schneier, 2003). Data is easy to collect, but it is the analysis that is the key component. Analysis makes the data useful and valuable. What United States intelligence agencies need is a better system for interpreting the data. Just as security systems are not truly tested until there is an attempt to make it fail, so with governmental intelligence, they tend to get public attention with a failure, not with the many success cases of detection and prevention.

Data that is used to provide security is restrained in democratic nations by the Constitutional right to privacy. In the United States ..."judges have had trouble regulating forms of electronic surveillance that don't clearly invade property rights" (Rosen, 2000). The Patriot Act has attempted to update legislation covering roving wiretaps and the electronic surveillance. The Court system is still sorting out how to define property rights with electronic surveillance and will be addressed later with regard to the Court's interpretation of the Patriot Act. Government does possess the following surveillance tools regarding the collection of data and information.

Surveillance Tools

Government uses the following surveillance tools: 1) subpoenas, 2) interception orders or wiretaps, 3) "pen register" and "trap and trace device" orders, and 4) search warrants. The Patriot Act has made the following changes to these surveillance tools.

Subpoenas, "which require a person to produce tangible evidence" are modified under Section 210 to allow for subpoenas to be issued "for records of electronic communications to include the length and types of services utilized, temporary network addresses, and the source of payment, including credit or bank card numbers" (Washburne, 2001). This is a significant expansion of powers regarding what types of information subpoenas cover, which used properly, allows for the successful prosecution of terrorists and criminals. However, if misused, this power has the potential to be a data mining experiment by the government and could potentially waste valuable time and resources chasing a rabbit down a hole.

Section 201 of the Patriot Act "adds terrorism to the list of offenses" that fall under the purview of wiretapping or interception orders that the government can pursue (Washburne, 2001). Providing support for terrorism was declared a criminal act in the 1996 Anti-Terrorism Act. The 1996 Anti-Terrorism Act included the "support for terrorism" provision, which made it ..."it a federal crime to support the legal activities of designated foreign terrorist groups" (Cole and Dempsey, 2002). The Patriot Act takes this a step further and allows for greater surveillance of terrorists beyond the former restriction, which required FISA court permission and was more narrowly defined.

Section 216 of the Patriot Act modifies the usage of pen registers to cover the collection of electronic mail and web-browsing information, but does not allow for the content of this to be gathered (Washburne, 2001). The information gathered from pen registers is useful to law enforcement because by capturing the phone calls made to other people and places, it helps authorities understand who the suspect talks to, which can lead to a better understanding of what the suspect's habits and associations are. However, if

electronic mail and web-browsing information can be gathered, then it will be very tempting to refrain from gathering the content, even if it is not allowable under law.

Pen registers and trap and trace devices identify the participants in a phone conversation and pinpoint the source and destination of telephone calls from the source (Doyle, 2002). "Pen registers are surveillance devices that capture the phone numbers dialed to outgoing telephone calls; trap and trace devices capture the numbers identifying incoming calls" (Center for Democracy and Technology, 2000). Section 214 does not allow for a pen register or trap and trace to be used for an investigation that is being performed solely on activities protected by the First Amendment (Washburne, 2001). Therefore, this governmental surveillance can not be conducted in such a manner that it poses a threat to the rights granted by the First Amendment, such as freedom of speech, press, religion, etc. Section 214, on paper, adheres to the principle of limited government that was so important to our Founding Fathers and to the legislation that arose from the Watergate experience that left Americans distrustful of government surveillance that trampled upon the right to privacy. The only problem with the restraint is, if surveillance can not be conducted that violates First Amendment rights, then how is this power being checked and how can violations be proven, if they are occurring?

Sections 219 and 220 address the long-standing issue of search warrants being able to be issued for only the judicial district issuing the warrant and instead, replaces this with search warrants that can be issued to cover the entire United States (Washburne, 2001). This change in search warrant jurisdiction is an essential tool to enable law enforcement and intelligence agencies to move quickly to capture terrorists who are in hot pursuit and still follow appropriate legal procedure. Under the previous rules governing search warrants,

time is a critical factor. The requirement of separate search warrants for each jurisdiction as the suspect moves from place-to-place made it extremely difficult, if not impossible, for law enforcement and intelligence agencies to apprehend suspects who posed a serious threat to American society and needed to be captured. However, the Constitutional question that the removal of the search warrant change raises is what has happened to due process? Once this barrier has been removed, will it be capable of being reinstituted if it has eroded due process?

This due process concern also applies to Section 209, which modified stored wire communication as being covered under the same rules as electronic communications, which use search warrant procedures. Prior to the Patriot Act, a wiretap order was needed to access stored communication, but a search warrant was needed to be used to gather information on a suspect's answering machine. Are these increased surveillance powers necessary or are there other solutions to provide better national security, such as data tagging, database integration and better analysis?

The best security will most likely come from increased tracking with data tagging, more time devoted to analyzing the data and training security professionals to watch for human behavioral cues, such as Israel is constantly training its security professionals to watch for. The data sharing entails ..."identification, authentication, and tracking of particular individuals who are known or suspected to be terrorists" (Yourdon, 2002). It also involves looking for patterns of behavior among individuals and groups to note activity indicative of some type of terrorist attack, such as chemical or biological. Criteria to analyze the data needs to be developed, which will assist with identifying ..."*patterns* of behavior and activity, in order to spot security threats either after they have occurred or (ideally) before they have occurred" (Yourdon, 2002). Just as private companies look for customer

trends, so should the government and intelligence conduct trend analysis for security breaches (Yourdon, 2002). Try to use a "honey-pot" approach to attract terrorists.

Database Integration and Analysis

There also needs to be better integration of databases and analysis of this information. The government has been attempting to integrate databases on tax collection, welfare and child support and law enforcement among federal, state and local agencies over the past 20-30 years (Yourdon, 2002). The challenges with integrating databases involve the individual agency culture and sense of defending that culture and territory. However, there are projects currently underway to accomplish such integration of governmental databases. The Pentagon is working to integrate its databases to develop a model for creating interoperable databases (Yourdon, 2002). President Bush created the President's Critical Infrastructure Board to consolidate and reorganize the government to prepare against a terrorist attack approximately four months before the September 11th attack. This was an attempt to build upon the Black Ice exercise, which tested the response of federal, state and local officials to a terrorist attack, as preparation for the 2002 Winter Olympics (Yourdon, 2002). The Patriot Act has sought to have government officials and private industry work together in cooperation by sharing information on suspected and/or actual terrorists.

This integration also includes greater sharing of information between the private sector and government. The private companies fear that such sharing of information may lead to this information being used by competitor companies, which will harm the company's profit margin. The government addressed this problem with the Protected Critical Infrastructure Information Program. "The PCII Program is designed to encourage private industry and others with knowledge about our critical infrastructure to share confidential,

proprietary, and business sensitive information about this critical infrastructure with the Government" (Protected Critical Infrastructure Information (PCII) Program, 2004). The idea behind the PCII Program is that the information can be shared with the government to be used solely for national security purposes and will not be publicly disclosed. Thus, the fear of use by competitors is eliminated by using the nondisclosure requirement.

In addition to the data sharing between and among government agencies and between the government and private industry, some global cooperation will also assist with sharing data, in terms of traffic analysis. "*Traffic analysis* is the study of communication patterns" (Schneier, 2000). Echelon is a global interception system, which is operated by the intelligence units from the United States, United Kingdom, Australia, New Zealand and Canada, which uses traffic analysis as it attempts to analyze the surveillance that it conducts (Schneier, 2000). Though some fear that the data and information collected by Echelon is a serious privacy violation, perhaps a united front of nations prepared to face terrorism head-on would help with the detection, identification, mitigation and/or prevention of terrorist attacks. It is this fear of expanded governmental power and the subsequent loss of privacy which is a primary concern with the Patriot Act.

CHAPTER THREE: EXPANSION OF POWER WITH THE PATRIOT ACT

In the wake of the September 11th terrorist attacks, both President Bush and Congress moved swiftly to tighten up the perceived security deficiencies that allowed terrorists to plan the attack for many years and then execute it without interference by United States security and intelligence services. The most direct response to these attacks was a massive new law referred to as the Patriot Act. The objective of this Act was to greatly increase the powers of the United States Government to gather, share, and act on domestic and foreign intelligence information. Legislation also created the Office of Homeland Security and the Critical Infrastructure Protection Board, an emergency supplemental spending bill and other measures to prevent against future terrorist attacks (Dacey, 2002).

The Patriot Act has sought to accomplish other improvements for preserving national security, such as modification of the Foreign Intelligence Surveillance Act. The Patriot Act has made some changes to the Foreign Intelligence Surveillance Act or FISA with the purpose of enabling law enforcement agencies to pursue and/or detain terrorists or suspected terrorists and/or spies in a more efficient and expeditious manner. Specifically, FISA has amended the timeline for electronic surveillance and physical search to enable law enforcement agencies to have the critical factor that significantly affects the successful investigation and detention of suspects, which is time. Section 151 of the Patriot Act, Period of Orders of Electronic Surveillance of Non-United States Persons Under Foreign Intelligence Surveillance, amends the Foreign Intelligence Surveillance Act of 1978, § 1805(e) (1) of title 50 or FISA "to extend the FISA court authorized maximum period for electronic surveillance of officers and employees of foreign powers and of members of international terrorist cells from 90 days to a year" (Patriot Act, 2001). This section also

amends FISA, title 50, § 1824(d) to extend the maximum period for a physical search of officers and employees of foreign powers and members of international terrorist cells from 45 to 90 days (Patriot Act, 2001). FISA 50 U.S.C. § 1804(a)(7)(B) and § 1823(a)(7)(B) regarding foreign intelligence information requires certification that "the purpose" of surveillance or search is to obtain foreign intelligence information (Patriot Act, 2001). One of the lessons learned from the September 11th attacks was that the Al Qaeda terrorists who planned this attack were very patient. Therefore, an extension of the time period for surveillance of foreigners and international terrorists would be a very important change that would greatly assist American intelligence. Likewise, an extension of the timeline allowed for physical searches of suspected foreigners and international terrorists would be another important consideration for assisting American intelligence.

Other expansions of governmental power with the Patriot Act include the modification of the FISA Act with regard to permission for law enforcement and intelligence to pursue in investigation. The certification for an order against a person engaging in espionage or terrorism can only be made at the written request of an official designated by the President and the Attorney General must *personally* review the application (Patriot Act, 2001). Section 153 of the Patriot Act amends FISA 50 U.S.C. § 1804(a)(7)(B) and § 1823(a)(7)(B) to change this standard requirement from the "sole and primary purpose" to "significant purpose" of the investigation (Patriot Act, 2001). Thus, the modification of the standard to significant purpose enables law enforcement and intelligence agencies to be able to move more quickly. If foreign intelligence can move more quickly, then it has a greater chance of apprehending and bringing to justice any and all suspects. However, does this expand the power of intelligence and law enforcement to a point where should this standard

be applied to domestic terrorism, it goes too far? (Electronic Privacy Information Center, 2001). Section 153 has the sunset provision that will expire on December 31, 2003, so perhaps this question will be answered when this report is due to Congress. This report has not yet been available to the public.

New Federal Crimes

To deal with the many different tactics employed by contemporary terrorists to attack a nation, the Patriot Act has defined new federal crimes to legally cover such actions. "The Act creates new federal crimes for terrorist attacks on mass transportation facilities, for biological weapons offenses, for harboring terrorists, for affording terrorists material support, for misconduct associated with money laundering already mentioned, for conducting the affairs of an enterprise which affects interstate or foreign commerce through patterned commission of terrorist offenses, and for fraudulent charitable solicitation" (Doyle, 2002). Thus, the Patriot Act seeks to be a more proactive response of the government to respond in a timely manner to the many different methods of terrorism that have changed with the rapid changes in information technology. For example, sections 201 and 202 of the Patriot Act add cybercrime and other terrorist crimes to the Title III of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996's predicate offense list (Doyle, 2002).

Congress has defined cybercrime as computer fraud and abuse involving "federal protected computers", which includes computers used or owned by the federal government, by a financial institution, or used in interstate or foreign commerce in 18 U.S.C. 1030 (Doyle, 2002). Section 814 of the Patriot Act increases the penalty for committing cybercrime. Thus, the Patriot Act defines new federal crimes, though many were mentioned in earlier laws, but were not adequately addressed in the wake of the new era of terrorism. The new

era of terrorism includes the use of Anthrax on mail to governmental officials and civilians as well as the significant network of money laundering and other forms of financial support that fund terrorist groups, like Al Qaeda. The Patriot Act accomplished the goal of bringing legislation up to date with new forms of terrorism. However, it does present some interesting issues with regard to the public policy debate of security versus privacy.

The Patriot Act is a comprehensive piece of legislation, which was passed shortly after the September 11th attacks. In terms of public policy, the Patriot Act has increased the domestic and foreign surveillance power of law enforcement and intelligence without making a strong distinction between them. Thus, the lines of distinction between what intelligence agents are allowed to gather on foreign terrorists and what domestic intelligence agent are allowed to gather have been blurred. Certainly strong leadership and action was necessary after the attack. However, the concern is that the swift response of the creation of the Patriot Act comes at the expense of American citizens sacrificing their Constitutional rights to privacy. It also generates the subsequent question of whether Constitutional rights have to be sacrificed to provide national security. Some would claim that better integration of the databases and analysis of the data and information are more effective in providing stronger national security.

American Tradition of Individual Privacy

In a democratic society that has extensive civil liberties protections, the issue of governmental intelligence gathering and surveillance is one of the most sensitive and important issues. Americans have prided themselves on having a strong legal tradition, based largely on the Bill of Rights that protects its citizens from overzealous governmental intrusion into their lives. This tradition has been strengthened by the long-standing suspicion

of a strong government that is reflected in the checks and balances and the efforts of the Founding Fathers to limit government. It is further reinforced by the American judicial philosophy that one is innocent until proven guilty. The burden of proof with criminal cases rests with the government, which must prove (through the presentation of legally obtained proof) that the defendant is guilty.

All of this has meant that Americans and, in particular, American civil liberties groups believe that it should be relatively difficult for the government to obtain private and confidential information, that individuals should have the integrity of their homes, mail, telephone conversations, cars, and personal body respected by law enforcement. In other words, the due process procedure makes it somewhat cumbersome for the police and intelligence services to tap into the privacy of people because the bar is set high to ensure that such evidence is obtained by legal and ethical means. These protections, however, came under scrutiny after September 11th, especially by the Bush administration and law enforcement agencies. They were seen by some as having made it difficult for law enforcement to gather and put together pieces of evidence to uncover the terrorist plot and/or arrest the terrorists before they could carry it out. On the other hand, critics of new, more intrusive, and harsher measures, such as the Patriot Act have argued that the existing laws were more than sufficient to have stopped the attacks. They argue that it was bureaucratic infighting, poor police work, under-funded agencies, and incompetence that led to the intelligence failure. Better management, competent communication and teamwork are the solutions to this failure of management, not the new harsher laws. The harsher laws are not only unnecessary, but are a threat to American civil liberties traditions.

The concerns of the critics of the Patriot Act are based upon concerns that the security measures pose a very serious threat to civil liberties and the right to privacy. Critics cite abuses of governmental surveillance from the past, such as the extensive wiretapping that was done with no regard for due process by former FBI Director J. Edgar Hoover as well as the Watergate scandal of the Nixon Administration. The Watergate experience led directly to the creation of the Privacy Act of 1974. However, to fully understand the importance of privacy, it is useful to take a look at its development from its inception in 1890.

Louis D. Brandeis, a Harvard law student who would later serve as a United States Supreme Court Justice, defined the right to privacy in an 1890 Harvard Law Review article as "the right to be left alone." (Alderman and Kennedy, 1995). The right to privacy finds Constitutional basis in the First Amendment, which "has a penumbra where privacy is protected from governmental intrusion." (Stone et al., 1991). By penumbra, the United States Supreme Court means "that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance." (Stone et al, 1991 (citing Douglas's dissent in *Poe v. Ullman*, 367 U.S. 497, 516-522)). Furthermore, those guarantees of the Bill of Rights create "zones of privacy." For example, the Fourth Amendment, which guarantees protection from illegal searches and seizures, falls within the zone of privacy in electronic communication (Prewitt et al., 2001). The search and seizure protection is most applicable to electronic surveillance, like domestic wiretapping, which Congress moved to more tightly regulate with the Privacy Act of 1974. The Privacy Act of 1974 establishes fair information practices as it pertains to personal information that is gathered and maintained by the United States government (Privacy and Electronic Communications, 2000).

The concern of critics with the Patriot Act and privacy is that the expanded surveillance granted for electronic and other forms of communication unduly infringed upon the private lives of citizens. The fear is that the increased power to conduct surveillance creates a climate where the bar is not set as high, which makes it easier for an abuse of government power. The subsequent concern is that once surveillance is expanded, it will be very difficult to erode such power, should serious violations to American citizen's privacy occur. Instead of repealing the entire Patriot Act, can we modify the surveillance sections of the Patriot Act to reach a better balance of enabling law enforcement and intelligence to be able to track potential and/or known terrorists, while preserving the Constitutional right to privacy?

Can We Modify the Patriot Act

Some sections of the Patriot Act are more controversial than others. As such, maybe one solution to the sweeping powers granted by the Patriot Act would be to scale such powers back. A second solution would be the role of the Courts in aiding in the interpretation of the Patriot Act and ruling if it has gone too far. One of the more controversial sections of the Patriot Act is the "sneak and peek" provision. Section 213, which is sometimes referred to as "sneak and peek" allows for a "reasonable period" of delay of notice that a warrant has been executed by the court, when such notice would possibly have an adverse effect on the pending investigation (Washburne, 2001). The "sneak and peek" latitude granted, again, seeks to address the need for law enforcement and intelligence agencies to move quickly, while still following appropriate legal procedure and not unduly interfering with a person's privacy. However, many believe that the "sneak and peek" section grants too much power to the government to conduct an investigation without

notification and thus, violates the system of checks and balances as well as the Constitutional right to due process.

In response to this concern, various legislative proposals, such as the Otter Amendment and the SAFE Act, which would modify the more controversial sections of the Patriot Act, have been proposed. However, such proposed legislation has not been introduced without resistance from the Justice Department. Indeed, there has been other legislation introduced, the Victory Act that would seek to offset any scaling back of the Patriot Act that the SAFE Act or Otter Amendment would accomplish.

The Otter Amendment is named after Representative C.L. "Butch" Otter (Republican-Idaho), who was the only member of Congress to vote against the Patriot Act. The Otter Amendment would remove funding for "sneak and peek" searches, but does allow delayed notification to the target of the search for a "reasonable" period (Schmitt, 2003). The Justice Department has voiced opposition to the Otter Amendment and has labeled it the "Terrorist Tip-Off Amendment". The Justice Department claims that removing funding for "sneak and peek" searches would thwart the efforts of law enforcement and intelligence officials to pursue and capture suspected terrorists. In early December 2003, the Otter Amendment died as it was not included in the omnibus spending bill by Congress. It did pass the House of Representatives before dying and Representative Otter has pledged re-introduction of his amendment in 2004.

The SAFE Act is the Security and Freedom Ensured Act. It is being supported by Senator Larry E. Craig (Republican-Idaho), Senator Richard J. Durbin (Democrat-Illinois) as well as members of the American Conservative Union, American Civil Liberties Union, Gun Owners of America, the Center for Democracy and Technology, and Electronic Frontier, etc.,

so it has support from both ends of the political spectrum, conservative and liberal. The SAFE Act has fours goals. First, the SAFE Act specifically limits the use of "sneak and peek" search warrants, which are warrants issued to allow searches of a target without notification " to situations where a life is at stake, evidence may be destroyed or there is a flight risk" (Hudson, 2003). Second, this bill would place limitations on the roving wiretap by requiring the suspect to be present when the wiretap is conducted on any phone the suspect is using (Hudson, 2003). Third, this bill also would reinstate the standards that were in existence prior to the Patriot Act, which govern how business and library records can be obtained by law enforcement. Prior to the Patriot Act, a grand jury subpoena was required to access this type of information. The Patriot Act removed the grand jury subpoena requirement and replaced it with a court order issued by a federal court, such as the Foreign Intelligence Surveillance Act (FISA) court. Fourth, the SAFE Act requires law enforcement agencies to have a court order to search library computers. The Patriot Act removed this requirement, which has been a concern among librarians and various Americans about the loss of privacy this power has created.

The Victory Act is officially called the Vital Interdiction of Criminal Terrorist Organizations Act of 2003. It contains several sections that resemble the Patriot II, which was an internal confidential document within the Department of Justice that was leaked to the press in February 2003 and encountered significant opposition from both liberals and conservatives. Officially, the Justice Department did not play a role in writing this legislation, which was sponsored by Senator Orrin Hatch (Republican-Utah). The Victory Act expands the government's power to investigate and prosecute drug dealers, narco-terrorist (terrorists that get their funding from engaging in drug sales), and money launderers

(Singel, 2003). In an attempt to address the problem of undocumented money transfers (hawalas), this bill also outlaws hawalas, which are used frequently in the Middle East, India and parts of Asia. Specifically, the Victory Act makes it easy for the FBI to obtain a wiretap order on a wireless device, gain access to financial records, and be able to conduct terrorism investigations without needing a subpoena issued from a judge (Singel, 2003).

The primary criticisms of the Victory Act are: 1) it blurs the distinction between the war on drugs and the war on terrorism, and 2) it grants too many police powers to law enforcement that are free to be exercised without the checks and balances that are a fundamental part of the framework of the Constitution. While a significant source of terrorist funding may be from illegal drug sales, there must be distinctions made between the different types of investigation that the FBI and other intelligence agencies conduct. Fundamental to the American system of government is that the United States has a written Constitution with an explicit system of checks and balances to provide safeguards to citizens regarding protection against excessive governmental intrusion into civil liberty areas, including the right to privacy. Perhaps the Courts will assist in the interpretation of the Patriot Act, which is one of its roles in the United States.

The Courts

Thus far, the Supreme Court has not issued decisions dealing with the debate over national security and privacy. It has however, made some rulings with regard to the Patriot Act. These rulings have stopped far short of calling into question the constitutionality of the Patriot Act. Time will tell if the Supreme Court will become more actively involved in the debate over national security and privacy with judicial interpretation of the Patriot Act.

The lower courts have issued some decisions regarding the Patriot Act. The most recent ruling regarding a section of the Patriot Act was made by a Federal District Court in Los Angeles on January 23, 2004. Judge Audrey Collins (a Clinton appointed federal judge) ruled for the plaintiffs in this case with regard to the section of the Patriot Act, which prohibits anyone from giving "expert advice or assistance" to known terrorist groups (Lichtblau, 2004). Judge Collins issued an injunction against the Justice Department to block it from enforcing this section of the Patriot Act on these plaintiffs. The rationale for this ruling was that this section was unconstitutionally vague and as such was in danger of violating the First Amendment. In her words, "The USA Patriot Act places no limitation on the type of expert advice and assistance which is prohibited, and instead bans the provision of all expert advice and assistance regardless of its nature" (Lichtblau, 2004). However, Judge Collins did not issue a national injunction on this section of the Patriot Act. Judge Collins did agreed with the Justice Department on other points of this case. This ruling may set a significant precedent as it is the first federal case in which a judge has struck down a part of the Patriot Act, even though it does not apply nationally (Lichtblau, 2004).

The Supreme Court has not currently become embroiled in the Patriot Act debate of national security versus privacy. Thus far, it has been supportive of the Patriot Act and the Bush Administration's handling of the war on terrorism by taking a stand of deference. It has refused to hear a few cases challenging the Patriot Act either on the basis of deference to the need for some national security measures to be kept away from the public eye and/or because a case has lacked sufficient Constitutional muster.

In January of 2004, the Supreme Court concurred with the ruling of a federal appeals court that the arrest and detention of people, mostly Muslim men, related to the September

11th attacks was allowable. The rationale for this decision was based upon an exemption to the Freedom of Information Act for "law enforcement records" (Greenhouse, 2004). This Supreme Court decision in *Center for National Security Studies vs. Justice Department* is consistent with the Court's ruling in 2003 regarding the challenge of closed session deportation hearings by the government used for the same people. Solicitor General Theodore B. Olson, in arguing for the government's ability to legally keep their files secret in this case, said "requiring the police to open their investigative files and provide a comprehensive list of the persons interviewed and detained—and by the same token to reveal which persons they have not interviewed and detained—would necessarily interfere with the investigation by providing a road map of law enforcement's activities, strategies and methods" (Stout, 2004). This is one of the many vulnerabilities with intelligence and law enforcement. When the data collection and technological tools used by law enforcement and intelligence are revealed to the public, it reveals too much information to the terrorists and criminals. Attorney General, John Ashcroft's response to the Court's decision on this case sums up this danger, when he states that he was "pleased that the court let stand a decision that clearly outlined the danger of giving terrorists a virtual road map to our investigation that could have allowed them to chart a potentially deadly detour around our efforts" (Greenhouse, 2004). The Supreme Court's ruling on these specific cases challenging the Patriot Act illustrate that the Court is recognizing the federal government's need to keep some aspects of their investigative cases out of public scrutiny. After all, intelligence needs to keep its data collection methodology, tools and information covert, so it can provide security.

On November 5, 2003, the Supreme Court declined to review a suit brought by the American Civil Liberties Union (ACLU) and other organizations on behalf of unnamed plaintiffs. The ACLU et al. were challenging the government's surveillance of people who were unaware that they were being monitored by the government. Such surveillance was granted by the Patriot Act's modification of the FISA court's ability to approve secret searches and wiretaps of suspected terrorists (Gaddy, 2003). For the Supreme Court to have heard such an unusual suit, it would have had to grant special permission for a suit brought for unnamed plaintiffs, who were not bringing the suit themselves. Thus, the reason for the Court's rejection of this suit without comment was most likely due to the lack of constitutional basis upon which this case was based and its highly unusual nature (Gaddy, 2003).

It remains to be seen whether any subsequent legal challenges of the Patriot Act will pass the Constitutional requirements of the Supreme Court to warrant being heard. Even if such a challenge would meet the Constitutional standard, it is dubious whether the Supreme Court will challenge the executive branch of government and strike down sections of the Patriot Act as being unconstitutional. Instead, the Court may continue to support the national security efforts of the Justice Department (executive branch) with the Patriot Act. Beyond the Courts, the 9/11 Commission may be able to offer some insight as to what contributed to the September 11th attacks. The Commission's findings may place the Patriot Act within a context to understand what parts of the Act address the inadequacies and what future action needs to be taken.

9/11 Commission

The report of the 9/11 Commission, which was created to investigate the terrorist attacks on September 11th, may also shed some light as to how necessary the Patriot Act is and may impact the Courts role. This commission has the potential power to reveal if it was a lack of communication, bureaucratic infighting and poor police work, which contributed to terrorist attacks taking place. Or was it a lack of power by intelligence, law enforcement agencies and Presidential Administrations to adequately meet the needs of national security, which the Patriot Act has sought to rectify?

Preliminary findings suggest that both the Clinton Administration and Bush Administration had warnings about the terrorist activities by Al Qaeda. The reason cited for the Clinton Administration's inaction was that they could not be brought to the United States without an indictment. The policy pursued was to try to convince the Taliban to expel Osama bin Laden to a nation which would extradite him to the United States (The Associated Press, 2004). The reason cited for the Bush Administration's inaction was that it was taking the time to review the Clinton Administration's ideas and plans. Thus, the Bush Administration was engaging in assessment and policy debate as Mr. Bush's aides found the Clinton Administration's plans and ideas to be lacking in effectiveness and overly narrow (Johnston and Purdum, 2004). Thus far, it appears that intelligence and specifically the CIA's counterterrorism center did pick up on suspicious activity, but it seemed to point to locations outside the United States. What does appear to be a problem was the ability of intelligence to adequately interpret warning signs and for intelligence to respond partially due to bureaucratic indecisiveness. The other problem is the lack of communication between intelligence and the Clinton Administration as to how define a decisive strategy for dealing

with Osama bin Laden and his terrorist organization, Al Qaeda. The Bush Administration took the time to analyze and try to assess how to handle Osama and Al Qaeda, which combined with conflicting ideas within intelligence created a situation where the September 11th terrorist attacks caught the United States by surprise. There are many lessons to be learned from this experience. The Patriot Act sought to apply some of the lessons learned. What remains to be seen is how successful the Patriot Act will be with this endeavor.

CONCLUSION

The Patriot Act is a comprehensive piece of legislation that has been controversial since its passage and subsequent signature into law in 2001. This act seeks to address serious cracks in our nation's armor with our federal agencies charged with protecting the nation from terrorist attacks. It has sought to address the new forms of terrorist crimes and related activities by defining them and making them prosecutable by the United States Government. The Patriot Act was enacted as the Bush Administration embarked upon a renewed effort to increase the information sharing between and among government agencies and between the government and private industry. As intelligence and law enforcement are seeking to better protect our nation from terrorist attack, they have the opportunity to assess how well the data processes work and determine if methods are available to make the data easier to analyze. Preliminary findings of the 9/11 Commission suggest the analysis of data is an area that needs improvement. Possessing data alone does not assist with the identification, detection and prevention of terrorism, but having the time, necessary tools and people to do the analysis to gain the necessary information from the data does. The expansion of power for intelligence and law enforcement with the Patriot Act is substantial. Congress, the Courts, the 9/11 Commission, and past experience will assist in assessing if this power expansion needs to be curtailed with a modification of the Patriot Act, such as the SAFE Act or if other remedies are needed.

The United States is not alone in its attempt to create legislation which updates the laws to include new forms of technology used by law enforcement and intelligence in its efforts to track and prosecute suspected and known terrorists and criminals. Great Britain passed RIPA in 2000, which expands the power of law enforcement and intelligence in areas

similar to the Patriot Act. France has recently passed Perben II, which increases surveillance power of law enforcement, like the Patriot Act and RIPA. Perben II also for the first time in French history is introducing the plea bargaining process, based upon the United States model. Thus, all nations are grappling with how to update the laws to reflect new forms of technological communication as well as how to provide better surveillance powers to law enforcement and intelligence to provide national security in an ever increasingly complex world of terrorism.

The effort of law enforcement and intelligence to protect a nation from terrorist attack is similar in complexity and scope to computer security, which is an ongoing process of constantly assessing the vulnerabilities and risks posed by adversarial and non-adversarial actors. Computer security is a continuous quest to develop software patches and updates to protect against unforeseen vulnerabilities. Likewise, with the ongoing efforts of intelligence agencies to protect against terrorism, the actors and their methods are constantly changing. The attacks of September 11, 2001 on the United States revealed some serious vulnerabilities with the assessment and communication processes possessed by intelligence, law enforcement, and two Presidential Administrations. The Patriot Act is one security update to solve some of these vulnerabilities. It will be a constant challenge to better assess the vulnerabilities and risks to design better updates and patches to prevent a similar attack in the future.

REFERENCES

Alderman, Ellen, & Kennedy, Caroline. (1995). *The Right To Privacy.* New York: Alfred A. Knopf.

Benjamin, Daniel, & Simon, Steven. (2002). *The Age of Sacred Terror.* New York: Random House.

Center for Democracy and Technology. (April 4, 2000). CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections [Web page]. Retrieved May 6, 2003, from the World Wide Web: http://www.cdt.org/security/000404amending.shtml

Cole, David & Dempsey, James X. (2002). *Terrorism and the Constitution: Sacrificing Civil Liberties In The Name of National Security.* New York: The New Press.

Combs, Cindy C. (2000). *Terrorism in the Twenty-First Century*, 2nd Edition. New Jersey: Prentice Hall.

Dacey, R.F. (2002, July 9). Statement on critical infrastructure protection: Significant homeland security challenges need to be addressed. Testimony presented to the Subcommittee on Oversight and Investigations of the House Committee on Energy and Commerce, 107th Cong., 2d Sess., Washington, DC. Retrieved November 9, 2002, from LexisNexis Database (Current Issues Universe, G014-121) on the World Wide Web: http://www.lexisnexis.com/ciuniv.

Doyle, Charles. (2002, April 15). The USA Patriot Act: A Legal Analysis. Congressional Research Service [Web page]. Retrieved November 12, 2002, from the World Wide Web: http://www.fas.org/irp/crs/RL31377.pdf.

Electronic Privacy Information Center. (September 24, 2001). Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001, Affecting the Privacy of Communications and Personal Information. Retrieved January 23, 2004, from theWorld Wide Web: http://www.epic.org/privacy/terrorism/ATA_analysis.pdf

Gaddy, Michael. (2003). Supreme Court Refuses to Hear Patriot Act Case. Sierra Times.com. Retrieved on November 5, 2003, from the World Wide Web: http://www.sierratimes.com/pf.php

Greenhouse, Linda. (2004). Supreme Court Roundup: Justices Uphold Policy of Silence on 9/11 Detainees. The New York Times, January 12, 2004. Retrieved on January 12, 2004, from the World Wide Web: http://www.nytimes.com/2004/01/13/politics/13SCOT.html

Henley, Jon. (2004). Lawyers Protest as French MPs give police more powers. The Guardian, February 12, 2004. Retrieved on March 31, 2004, from the World Wide Web: http://www.guardian.co.uk/france/story/0,11882,1146152,00.html

Herman, Michael. (2001). *Intelligence Services in the Information Age*. Oregon: Frank Cass Publishers.

Hudson, Audrey. (2003). Senators join forces to roll back parts of Patriot Act. The Washington Times, October 16, 2003. Retrieved October 29, 2003, from the World Wide Web: http://www.washtimes.com/national/20031016-120041-3361r.htm

Johnston, David, & Purdum, Todd S. (2004). Missed Chances in a Long Hunt for bin Laden. The New York Times, March 25, 2004. Retrieved on March 25, 2004, from the World Wide Web: http://www.nytimes.com/2004/03/25/politics/25HUNT.html

Lichtblau, Eric. (2004). Citing Free Speech, Judge Voids Part of Antiterror Act. The New York Times, January 26, 2004. Retrieved on January 27, 2004, from the World Wide Web: http://www.nytimes.com/2004/01/27/politics/27PATR.html

Prewitt, Kenneth, Allen, Anita L., Berman, Jerry, & Bruening, Paula, Cohen, Jean L., McGovern, Theresa M., Scarf, et al. (2001). Is Privacy Now Possible? A Discussion. *Social Research*, 68 (1), 297-338.

Privacy and Electronic Communications. (2000). Hearing Before the Subcommittee on Courts and Intellectual Property of The Committee on The Judiciary House of Representatives (Serial No. 86). Washington, DC: U.S. Government Printing Office.

Porch, Douglas. (1995). The French Secret Services: From the Dreyfus Affair to the Gulf War. New York: Farrar, Straus and Giroux.

Protected Critical Infrastructure Information (PCII) Program. (2004). United States Department of Homeland Security [Web page]. Retrieved March 27, 2004, from the World Wide Web: http://www.dhs.gov/dhspublic/display?theme=31&content=3228

Provide Appropriate Tools Required To Intercept and Obstruct Terrorism (PATRIOT) Act of 2001, 107th Cong. (2001).

Risen, James. (2003). Ex-Government Officials Recommend Intelligence Overhaul. The New York Times, December 8, 2003. Retrieved December 9, 2003, from the World Wide Web: http://www.nytimes.com/2003/12/09/politics/09TERR.html

Rosen, Jeffrey. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.

Schmitt, Richard B. (2003). Why War? Planned Patriot Act II Losing Audience. why-war.com, July 29, 2003. Retrieved October 29, 2003, from the World Wide Web: http://www.why-war.com/news/2003/07/29/plannedp.html

Schneier, Bruce. (2000). *Secrets and Lies: Digital Security In A Networked World.* New York: John Wiley & Sons, Inc.

Schneier, Bruce. (2003). *Thinking Sensibly About Security in an Uncertain World.* New York: Copernicus Books.

Sciolino, Elaine. (2004). Lawyers Protect Across France at Sweeping Anticrime Law. The New York Times, February 12, 2004. Retrieved February 18, 2004, from the World Wide Web: http://www.nytimes.com/2004/02/12/international/europe/12FRAN.html

Singel, Ryan. (2003). Patriot Act II Resurrected? Wired News, August 21, 2003. Retrieved October 29, 2003, from the World Wide Web: http://www.wired.com/news/politics/0,1283,60129,00.html

Stalder, Felix, & Hirsh, Jesse. (2002, June). Open Source Intelligence. *First Monday*, 7 (6). Retrieved on April 23, 2003, from the World Wide Web: http://firstmonday.org/issues/issue7_6/stalder/index.html.

Stone, Geoffrey R., Seidman, Louis M., Sustein, Cass R., & Tushnet, Mark V. (1991). *Constitutional Law.* Boston: Little, Brown and Company.

Stout, David. (2004). High Court Won't Review Terror-Captive Secrecy Case. Arizona Central.com, January 13, 2004. Retrieved January 28, 2004, from the World Wide Web: http://www.azcentral.com/arizonarepublic/news/articles/0113terror-scotus13.html

Strange, Susan. (1988). *States and Markets.* London: Printers Publishers.

The Associated Press. (2004). 9/11 Panel Cites Clinton, Bush Inaction. The New York Times, March 23, 2004. Retrieved on March 23, 2004 from the World Wide Web: http://www.nytimes.com/aponline/national/AP-Sept-11-Commission.html

The Regulation of Investigatory Powers Act (RIPA). (2000). Crime and Policing [Web page]. Retrieved March 28, 2004, from the World Wide Web: http://www.homeoffice.gov.uk/crimpol/crimereduc/regulation/

Washburne, Thomas W. (2001). Summary and review of anti-terrorism legislation: The PATRIOT Act of 2001. Retrieved November 9, 2002, from LexisNexis Database (Current Issues Universe, A146-11) on the World Wide Web: http://www.lexixnexis.com/ciuniv.

Yourdon, Ed. (2002). *Byte Wars: The Impact of September 11 on Information Technology.* New Jersey: Prentice Hall.