The Patriot Act – An Impact Analysis

Dr. Paul Jorgensen

Carol Capek Sam Gustafson Jason Kadzban Donalyn Sandborn

11 December 2003

Department of Computer Science and Information Systems Grand Valley State University 1 Campus Drive Allendale, MI 49401 USA

Table of Contents

- I. Introduction
- II. Definition of the Issues
 - a. Issues with Clarity & Definition with the Law
 - b. Impacts of the Law on Computing
 - Training
 - Customer Identification Program
 - List Management
 - Integration of Data
 - Responsibility
 - Surveillance/Electronic Monitoring
 - Foreign IT personnel and Students
 - Internet
 - Data Security
- III. Compliance/Regulatory Impacts to Business
 - a. Financial Institutions
 - 1 Businesses that are Affected
 - 2 Penalties for Non-Compliance
 - 3 How Companies Become Compliant
 - In-House Solution Insurance Company
 - Outsource Solution Credit Union
 - 4 Feasibility of Compliance
 - b. Internet Service Providers
 - 1 Surveillance
 - 2 Carnivore
 - 3 Client Information an ISP Can Provide to Law Enforcement
 - 4 Clarity of Expectations
- IV. Opportunity/Growth Impacts to Business
 - a. Overview of Businesses and Growth of Sales
 - b. Companies
 - Mantas
 - CAPPS II
 - CRM Solutions Searchspace
 - c. Compliance
 - d. Foreign Country Needs Sybase

- e. Consulting, Project Management, and Training
- f. Data Mining
- V. Government Impact
 - a. Local, County, State, Government/Agencies Impacts
 - 1. Local & County Police Impacts
 - 2. Library Impacts
 - 3. Resolutions by Cities to Monitor
 - 4. Resolutions by Cites to Oppose
 - 5. State Impacts
 - b. Federal Governments/Agencies Impacts
 - 1. Government-Supplied Lists
 - 2. Information Sharing
 - 3. Integrated Entry and Exit
 - 4. Border Control
 - 5. Financial Monitoring
 - 6. Control Processes
 - c. Universities and Schools
- VI. Conclusions
- VII. Works Cited
- Appendix A Description and Overview of selected sections of the USA PATRIOT Act
- Appendix B Information Technology Aspects of Patriot II
- Appendix C Author Information
- Appendix D Assigned Sections

I. Introduction

This paper concludes the Capstone Seminar for the Master of Science degree in Computer Information Systems for Fall 2003 at Grand Valley State University. Four participants along with Professor Paul Jorgensen, Ph.D., analyzed the implications of the USA PATRIOT Act upon computer information systems, information technology, and associated processes. Appendix A has a brief, non-legal, description of pertinent sections of the USA PATRIOT Act; Appendix B has a description of the new Domestic Security Enhancement Act, commonly known as Patriot II; and Appendix C has a brief selfdescription of each participant.

The Capstone Seminar is an integrative course in which students lead a discussion and present a paper on a current topic. In addition, the Capstone Seminar promotes collaboration among graduate students and gives both faculty and graduate students an opportunity for sustained work on topics outside the scope of regular course offerings.

On October 26, 2001, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act - commonly known as the USA PATRIOT Act. For the purpose of this paper, it will be referred to as the Patriot Act.

There are several different views on this Act. Some critics feel it was recklessly and hastily pushed into law due to the hysteria surrounding the September 11 terrorist bombings. A vast majority of sections in the Patriot Act could not have been carefully studied by Congress, nor was sufficient time taken to debate it or to hear testimony from experts outside of law enforcement in the fields where it makes major changes. This concern is amplified because several of the key procedural processes applicable to any

other proposed laws, including inter-agency review, the normal committee and hearing processes and thorough voting, were suspended for this bill. [28] Proponents of the law feel that we have given sweeping new powers to both domestic law enforcement and international intelligence agencies to improve our security and that those measures are needed at any cost. In general, with the Patriot Act in place, they feel more secure flying or traveling to larger cities, feel our borders are better protected, and feel the information sharing among government agencies is creating a more thorough process to "weed-out" the terrorists working against the United States and its citizens.

The Patriot Act has created a number of industry-specific regulations that have been implemented to govern how companies control and protect their business systems within their enterprise and across subsequent partner, supplier, and customer chains. Regulations target companies within different industries; however, the main thrust of the mandates is quite similar. All of the regulations strive to improve the way data is managed and protected within information systems, in order to allow businesses to enhance corporate accountability, ensure data integrity, mitigate risks, and streamline operational efficiencies. Companies need to know with whom they are doing business. In some cases, the Patriot Act has created a new position within organizations – the Compliance Officer. The Compliance Officer is the person ultimately responsible for a company meeting all the requirements of the Patriot Act and any other mandates for doing business. Up to this point, only larger businesses impacted by many laws and regulations had a comparable position to manage such information and assure the company's compliance.

The Patriot Act is 342 pages long and makes changes to over 15 different statutes. It contains a number of provisions that propose closing the information-sharing gaps between different government agencies. Some feel that this will create an Orwellian "1984" atmosphere where the government monitors and controls every aspect of individuals' lives. Others feel it is long past due. Most agree that it brings up the question of who should have access to this data and who is monitoring the individuals with access to this data.

Computing professionals should pay careful attention to the Patriot Act. Most obviously, compliance to the Patriot Act will form the basis of political and fiscal support for initiatives that might or might not be technically feasible. For example, if an Internet Service Provider (ISP) were to keep a record of every website their customers visited for an indefinite period of time, this would require huge amounts of storage space and additional manpower. For an ISP to undertake such a project would not be feasible; it would be an unjust burden. Hastily devised strategies fueled by the expedience and convenience of our congress may well have escaped the rigor of full technical scrutiny. Perhaps more important is the likelihood that any wide-scale plan for interoperability, data sharing, or redrafted platform standards will have a lasting implication for generations of future technologists. The political motivation for such reforms may not be technically feasible, in which case everyone suffers unintended consequences for more than just our generation. If we do not get it right, we could be creating a huge headache for posterity.

On the bright side, if a company complies with its own definition of the Patriot Act, it is now considered to be a Patriot. The Patriot Act is viewed as an evolution and a

revolution depending on the stand that is taken. Many of the provisions in the Patriot Act only have a four-year term at which point they sunset (expire). Other provisions are permanent. Additionally, a Patriot Act II is in the works to refine and address additional areas of control.

This document will focus on the effects the Patriot Act has had on the compliance and regulatory impacts to businesses, the opportunity and growth impacts to businesses, and the government impact.

II. Definition of the Issues

Issues with Clarity & Definition with the Law

The Patriot Act introduced sweeping changes to U.S. law, including amendments to:

- <u>Wiretap Statute</u> (Title III)
- <u>Electronic Communications Privacy Act</u>
- Computer Fraud and Abuse Act
- Foreign Intelligence Surveillance Act
- Family Education Rights and Privacy Act
- Pen Register and Trap-and-trace Statute
- Money Laundering Act
- Immigration and Nationality Act
- <u>Money Laundering Control Act</u>
- Bank Secrecy Act
- <u>Right to Financial Privacy Act</u>
- Fair Credit Reporting Act

The Patriot Act is vague and difficult to follow. This one Act actually amends dozens of existing laws. For the Patriot Act to make sense, one needs to refer to multiple Acts. Overall, this hastily passed legislation is obscure and will fuel significant ramifications. As such, this paper offers no quick index of what is required under the new law. Moreover, one of the real burdens of this new law is that Compliance Officers along with business lawyers will have to make sense of it on their own until precedents have been established in the courts.

One provision of the new law requires companies to report "suspicious transactions" to law enforcement. This precipitates a host of questions: Does this mean organizations must monitor activity like email and Internet web browsing---and to what degree? If this means keeping logs and archiving such activity, how long shall it be kept? Does information contained in systems logs at universities, colleges, and schools constitute education records? If our government is combining databases and going to be doing data mining, how are they going to keep themselves from violating Federal Laws that prohibit profiling?

Currently, no precedent exists defining how these laws will be applied in the real world, and who knows what constitutes "suspicious." In response to the Patriot Act, the easiest rule of thumb is to know whom you conduct business with and to maintain records of all business dealings. Consequently, this may strengthen business practices --- even if the primary business objective is not trying to identify terrorists.

United States Foreign Intelligence Surveillance Court (FISC) judges are allowed to obtain records on Americans in support of an international terrorism investigation; at

the same time, the judges may not compel production of records concerning First Amendment activities. Who is defining the difference between First Amendment activities and terrorism? If a U.S. citizen views an anti-congress website that a known terrorist has also viewed, is that a terrorist activity or a First Amendment right? As another example, consider if an individual were on a flight that a suspected terrorist was on as well. Does this automatically give FISC judges approval to have the FBI search the government database on the individual and request data on the individual from any company that may have a record pertaining to that person? Is travel a First Amendment right only if the individual does not cross the path of suspected terrorists? With our government's past flawed record of power abuses, this is dangerous because someday perhaps an individual's voting pattern may qualify that person as a likely terrorist.

The Patriot Act is still in the nascent stage, lacking concrete definition. For example, consider section 326, which deals with banking. It keeps broadening in regard to affected industries. To date, the defined industries include banks, credit unions, futures commission merchants, futures introducing merchants, mutual funds, thrifts, trusts, and securities dealers. This list is not yet finalized. Section 326 of the Patriot Act deals with financial institutions needing to know whom they do business with. This requires them to verify the identity of any customer seeking to open an account but excludes a person with an existing account, provided their identity is "reasonably" known. To date " reasonably known" is determined by each individual institution. Thus one bank may count any current customer as "reasonably known," and another bank may count a person with a local address and phone number as "reasonably known." In some cases, perhaps nobody is considered "reasonably known," thus requiring an ID. This area is getting particular

attention because it helps with examining money flowing in and out of accounts to prevent money laundering and ensuring adherence to know-your-customer rules, which are thematic throughout the Patriot Act. Again, each company has its own definition of what constitutes evidence of money laundering, and they are all slightly different.

To summarize, the clarity and definition of the Patriot Act is ambiguous. It can be used and interpreted in many different ways. To be safe, legal interpretation is advised. Until more cases are brought to court under the guise of the Patriot Act, the clarity and definition of particular sections will remain vague. And, this vagueness remains a critical issue.

Impacts of the Law on Computing

<u>Training</u>

Many companies now use Information Technology (IT) to spot possible criminal activity. Larger banks, especially, spend millions on software that watches for suspicious transactions and unusual patterns. Information Technology departments will need more training on the security side of business as opposed to the computing side. Compliance with these new regulations and standards inherent in the Patriot Act will also take additional training of IT project managers. These regulatory compliance efforts are IT intensive and may lead to a resurgence of training for IT personnel. After Y2K bug scare, as a cost saver for companies, most IT project management training stopped. Meta Group Inc. issued a report in July 2003 which states that less than 15 percent of companies polled informally have IT project management training programs in place. Many firms are now using E-learning programs to train employees on compliance issues. [106] If, as

so many articles have stated, technology is the key to compliance, then companies should be investing in training IT personnel.

Customer Identification Programs

Financial institutions are required to develop and maintain a risk-based approach to a Customer Identification Program (CIP). As of October 1, 2003, financial institutions needed to have in place a system for customer identification, verification, record keeping, customer notice, and data list screening. That goal allows for taking many current "know your customer and due diligence" procedures already in place at most institutions and cross-applying them to Section 326. Financial institutions began section 326 compliance by doing an inventory of current practices for anti-fraud measures and examining the tools used in that capacity and then repackaging these for their own CIP practices. Financial institutions that did not have all these measures in place had to either modify their systems or purchase off-the-shelf software.

List Management

The U.S. has always published a Denied Parties list of entities from which U.S. companies are prohibited from engaging in business. Over time the list has changed only sporadically, but since the Patriot Act, this list and others change daily. Lists include Denied Persons, Embargoed Countries, and International Traffic in Arms Debarment. The U.S. General Accounting Office (GAO) agrees that these lists of suspected or known terrorists create an undue burden on those bound to heed them. In a summary of its report GAO-03-322, the GAO wrote, "Nine federal agencies - which prior to the creation of the Department of Homeland Security spanned the Departments of Defense, Justice, State,

Transportation, and the Treasury - develop and maintain 12 watch lists. These lists include overlapping but not identical sets of data, and different policies and procedures govern whether and how these data are shared with others." [107] Differences in the systems' architecture of various government agencies impede efficiency and optimization in sharing data.

Integration of Data

The Patriot Act mandates the detection of certain types of suspicious banking activities. The Patriot Act sections that pertain to this and the reports that need to be filed with the government are very complex. Nefarious banking customers have skirted Bank Secrecy Act provisions in the past by clouding their activities. For example, they might break up large transfers to one person over several days and several bank branches. Exposing this behavior requires integrated data and automated detection. In regard to all the new sections of the Patriot Act pertaining to surveillance, an issue is where will all the collected data be stored and who will have access to that information? These details are unclear.

Responsibility

It takes effort to monitor and ensure that a firm is compliant with the Patriot Act, and this mandate forces someone to be responsible at a senior level, i.e., usually now referred to as the Compliance Officer. The increased onus on compliance officers will force them to explore technology tools to assist in meeting the increased demands. "As business has gotten more complex and rules more stringent, we really need technology to ensure we're in compliance," said Dave DeMuro, managing director at Lehman Brothers

and director of global compliance and regulation. "The sheer volumes that we deal with are so great that the only way we can come close to knowing what is going on at the firm is to avail ourselves of technology." [76] The new technology will have to be implemented and controlled by the Compliance Officer. There is only so much that technology can accomplish, and it can not stop everyone intent on deception and/or malice. IT departments can only establish reasonable standards and supervision of systems, knowing there will always be a "bad apple" who may intentionally choose to violate laws and regulations.

A second area of responsibility is especially important for network operators. The government has new powers to subpoena electronic records and monitor Internet communications, and operator assistance may be required. This will be old news for those working for a major ISP or backbone operator. Most have already been visited and made decisions on how to cooperate with government investigators. As investigations move from high-traffic areas to more specific places on the network, even small ISPs, bulletin board operators, list administrators, and IT managers may start receiving calls from government officials. Network operators will want to consider well in advance what to do and know what the law requires---before they get a call.

Cheerfully accommodating a new customer named John Doe is no longer acceptable. Reasonable steps will need to be taken to verify the identity of customers, and the verification documents will need to be filed. In addition, customer names will need to be checked---both individuals and organizational names---against a list of known and suspected terrorist organizations. If a match occurs, the compliance officer has a duty to report the person or organization to law enforcement.

The new laws also focus on cash and wire transfers. For example, whenever cash is handled in excess of \$10,000 in any single transaction, businesses have to report the transaction to government officials. This is not a big deal for most businesses, but for the manager of a casino, this could prove to be an administrative nightmare. Furthermore, the Treasury Department has extended anti-money-laundering rules to jewel traders and opened discussions on applying them to auto dealers and travel businesses, all industries that handle large monetary transactions. [25] For most Internet-related businesses, those that do not handle cash at all, requirements to maintain records of wire transfers and other electronic transactions pose similar burdens.

Surveillance/Electronic Monitoring

The Patriot Act endows law enforcement with new surveillance powers. Many of the revisions were designed to bring the Internet, voicemail recordings, wireless voice and messaging services, and other new forms of electronic communications within the scope of existing search and seizure laws. It modernizes the 35-year old Federal Wiretap Statute to consider cell phones and the Internet, which are communication technologies that did not exist in 1968 when that statute became law. Every kind of informational medium is now subject to government search and seizure. For information companies, this includes live systems, back-ups, and archives. It means that information traveling through routers and servers is subject to monitoring without user knowledge.

One aspect that is really new and different is the delayed notice provision for certain kinds of search warrants. Under the Patriot Act, the government is allowed to collect information first, and then give notice of what it has done later. Typically, when a

search warrant is issued, the person whose property is about to be searched is given notice. Not so under the new Patriot Act. In circumstances when the government is afraid that a search warrant will alert a suspect to the surveillance and give him or her the chance to flee, the government can search first---and inform later.

The business justifications for employer monitoring have been bolstered by their relationship to national security concerns. Both employers and employees have mutual interests in promoting national security, but they also have mutual privacy concerns that arise from the recent development of laws related to electronic monitoring. This is because federal laws designed to facilitate electronic monitoring for national security purposes empower law enforcement to conduct electronic monitoring in new ways that may impact the privacy of both individuals and businesses.

Three types of electronic monitoring prevail. First, it includes employer use of electronic devices to review and measure the work performance of employees. For example, an employer may use a computer to retrieve and review an employee's email messages sent to and from customers in order to evaluate the employee's performance as a customer service representative. Second, it includes "electronic surveillance" in the form of employers' use of electronic devices to observe the actions of employees while they are not directly engaged in the performance of work duties, or for a purpose other than to measure their work performance. For example, an employer may electronically review an employee's email messages as part of an investigation of a sexual harassment complaint. Third, it includes employer use of computer forensics, the electronic recovery and reconstruction of electronic data after deletion, concealment, or attempted destruction of the data. For example, an employer may use specialized software to retrieve or recover

email messages stored on the employer's computer hard drive that relate to an investigation of alleged theft of its trade secrets by an employee. [55]

One way for an employer to obtain the consent or authorization of a user to intercept or access stored electronic communications is to adopt and distribute a workplace policy permitting the employer to electronically monitor employee electronic communications in the workplace. To take advantage of this statutory exemption to shield the employer's electronic monitoring of communications by employees in the workplace, an employer needs a comprehensive workplace policy that has been communicated to employees. Alternatively, the employer could obtain individual consent from employees for the employer's electronic monitoring. The federal privacy statutes have been recently amended by Congress in the Patriot Act and have important implications for employers. Also recent federal circuit and district court cases have interpreted the scope of the laws narrowly, avoiding unnecessary restrictions on the use of electronic monitoring by employers or law enforcement. The combined actions of Congress and the courts have effectively expanded the ability of employers to monitor electronic communications of employees without violating these laws. However, there are negative implications for businesses as well. These arise from recent developments and include enhanced ability of law enforcement to compel businesses to monitor their electronic communications systems for law-enforcement purposes and enhanced government access to electronic communications by businesses. [55]

Service providers have expanded obligations under the Patriot Act. For example, the definitions of trap-and-trace device have been significantly expanded to allow for access to certain information (excluding content) concerning Internet activity. Another

example is the obligation to respond to a nationwide service of process that in some instances may not identify the company on the face of the service document. The Patriot Act does permit persons to seek clarifications.

The Patriot Act contains three favorable features for communications companies. First, it provides specifically that nothing in the Patriot Act creates any new requirements for technical assistance, such as design mandates. Therefore, the right, if any, of the government to require use of design mandates or other technical assistance by service providers is not affected or augmented by the Patriot Act. Second, in several important areas, the Patriot Act expands service provider protections including immunities and good faith defenses for complying with new or existing surveillance authority, as is the case in FISA wiretaps and disclosures of records. The Patriot Act also creates expanded ability for the government to conduct wiretaps, at the request of service providers, of hackers and other "trespassers" on service provider networks. Third, the Patriot Act amends and limits the Cable Act to make it clear that companies offering cable-based Internet or telephone service will be subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only where detailed cable viewing information is being sought. In all other instances, cable operators offering these services can respond to a government surveillance request under the Electronic Communications Privacy Act, which does not require service providers to notify subscribers of requests. [20]

Foreign IT Personnel & Students

Another burden on Information Technology companies is likely to come as a result of revised immigration and visa procedures. Throughout the dot-com boom, companies lobbied Congress fiercely for increased access to foreign technical workers, including an increase in the number of work visas that would be permitted. While the demand for talent has decreased over the last year, the process of getting foreign workers into the United States on visas will probably become more complicated and more time-consuming. The same holds true with foreign students capacity to obtain and maintain their student visas.

Companies located in foreign countries that do business with the United States will have to abide by the Patriot Act as well. Furthermore, the routine business trips into this country by foreign business partners and customers are likely to be more difficult. Anecdotal evidence abounds that visitors to our country are often greeted by long lines, invasive searches, and, with increasing frequency, lengthy investigative detentions. Some companies have decided to make visits overseas, rather than have important business contacts subjected to the heightened security and immigration practices that will greet them here.

<u>Internet</u>

The Patriot Act defines, in section 217, a "computer trespasser" and improves the government's ability to track them over the Internet with assistance of ISPs. The Patriot Act promotes the use of security on the Internet to help facilitate the integrity of the data. Section 210 expands the amount of information that can be requested from an ISP by

government officials. Section 211 places Broadband Cable companies that are providing phone and Internet service under the same guidelines as those of an Internet Service Provider. Sections 216 & 220 allow surveillance techniques to be used to monitor Internet usage of suspected terrorists with a court order from anywhere in the United States. Internet Service Providers and even an employer that provides Internet access to employees is now required to turn over usage records and help set up the real-time monitoring hardware the FBI uses, called Carnivore, if ordered. Section 808 adds certain computer fraud and abuse offenses to the list of violations that may constitute a federal crime of terrorism. These offenses could be perpetrated with use of the Internet. In section 814 the previous penalties were doubled and what constitutes "damages" and how it is calculated are defined. Expenditures of \$50 million to develop and support regional cyber security forensic capabilities are authorized in section 816. If our Administration deems the Internet as a critical infrastructure to our country, like our electric grid, then it also will be covered under Section 1016 that covers infrastructure protection and continuity through support for activities related to counter terrorism. This section establishes the National Infrastructure Simulation and Analysis Center (NISAC) to address critical infrastructure protection and continuity.

Data Security

Section 701 calls for the Department of Justice establishment of a secure information-sharing system. It does not stipulate if it should be the government doing the work to make the data secure or whether it should be outsourced to a private company to guarantee data security. With the conversion of many databases to a few, there will be large access to the few databases that remain. Heavy reliance on centralized databases

with wider access by more users will require careful attention to data protection and the authentication of users. One way this may be achieved is through the use of public key infrastructure (PKI) encryption systems. PKI systems are generally considered the most reliable means to ensure the security of online transactions. However, implementing a PKI system can be a very difficult, time consuming, and expensive process. Moreover, in the case of federal government projects, the PKI systems used by different departments and agencies would need to be interoperable in order to realize the efficiencies hoped for, and convenience necessary, to achieve the desired citizen usage levels. So far, no such standards have been established. The challenge of establishing a large-scale PKI system raises many issues. Some of these include the lack of federal interoperable standards, the feasibility of implementation, and high costs. [13] Implementation of such a system would require policy makers to decide if the federal government has sufficient expertise and resources to create a large scale PKI system in-house, or if it will need to be outsourced to one or more private contractors. The largely uncharted nature of such an undertaking along with the high costs of PKI systems generally, raises concerns for budget planning and oversight. Proponents of a government-wide PKI system maintain that if these issues can be adequately addressed, the creation of a single government-wide PKI system could promote the utilization of secure Web portals to ensure the data integrity of transactions between the government and citizens and business.

III. Compliance/Regulatory Impacts to Business

Financial Institutions

This section will look at different impacts on business with special attention given to insurance companies, credit unions, and Internet service providers.

Businesses that are Affected

The Patriot Act has without a doubt brought about a substantial increase in the legwork many companies must undertake to be in compliance. However, while the Patriot Act is very significant in terms of "what" companies must do; it is at least as significant in terms of "who" must now do it. For instance, financial institutions are the primary target of Patriot Act regulations. Prior to this legislation, reference to such institutions primarily meant the banking industry. As a result of the Patriot Act, the term "financial institution" now is much more encompassing, referring not only to banks, but also to many other types of businesses as well. [90]

As one example, automobile dealerships now have additional requirements resulting from the Patriot Act. On occasion, the Federal Treasury Department's Financial Crimes Enforcement Network (FinCEN) may have reason to request information from a dealership regarding a particular individual or entity. In such instances, the dealership must search for and turn over any records relating to an account held by the individual or entity within the past year. In addition, the dealership must also produce any transactions made with the individual or entity within the past 6 months. [12] Moreover, the term "financial institution" now includes casinos with annual gaming revenues of at least \$1 million. Such casinos are required to file a Suspicious Activity Report with FinCEN for

any transactions conducted therein amounting to at least \$5,000 and that meet certain criteria for suspicion. [37] The Patriot Act also expressly identifies insurances companies and jewelers who buy or sell in excess of \$50,000. Such entities are required by the Patriot Act to establish anti-money laundering programs. [38] [69] As a final example, in a former job I worked for a large retailer. This company had to develop procedures for Patriot Act compliance because it issues money order transactions. The company did not automate their money order process at all. However, with the advent of the Patriot Act, the company now must monitor its money order transactions for suspicious activity, whether it occurs at one store or over several stores.

In reality, all business entities could now fall under Patriot Act scrutiny, as every business ultimately transacts money with people or other businesses. Therefore, whether or not it is explicitly noted in the Patriot Act's definition of a financial institution, each and every business should assess what it needs to do to comply.

Penalties for Non-Compliance

In the current business environment, Patriot Act compliance is not an option; it is a must. Penalties for non-compliance are indeed severe. The Federal government may assess companies criminal penalties of up to \$1 million *per incident*. Civil fines of \$250,000 per incident may be assessed as well. Executives may also be fined and even imprisoned depending on the severity of the violations. Forfeiture of accounts and other assets in question is another possible penalty. Perhaps even more threatening than these penalties is the potential impact of negative publicity that would arise from a company being cited for violations. [87] Although it is not yet perfectly clear as to exactly what and how much companies must do to avoid these fines, recent cases involving Western

Union and PayPal make it clear that these potential fines and prosecution are more than mere idle threats.

First of all, money-transfer giant Western Union recently had to pay out \$11 million: \$3 million for a civil penalty to FinCEN and \$8 million in fines to the State of New York, in relation to violations of the Patriot Act. The violations were of the Bank Secrecy Act (BSA) stipulation that currency transactions of over \$10,000 by an individual must be reported. This provision of the BSA has been in place for several years for banks and now, due to the Patriot Act's broadening of the definition of financial institutions, applies to Western Union.

Western Union was not altogether ignoring the Patriot Act requirements. It had been identifying and reporting multiple transactions totaling over the \$10,000 limit made by an individual during the same day through the same Western Union agent. However, after a nationwide review done by Western Union as requested by FinCEN, it was determined that the company was not identifying and reporting multiple transactions totaling over the limit conducted at different agents or over different business days. FinCEN ruled that these lapses constituted violations of the Patriot Act.

In addition to the fines and penalties, Western Union had to file 662 additional suspicious activity reports as a result of the review. Also, Western Union agreed to make enhancements to its systems so as to avoid such lapses in the future. This example underscores the technological burden that the Patriot Act may place on many companies. It is very likely that many large companies, like Western Union, perceived little or no need in the past for their information systems to compare each transaction with every other transaction made nationwide or even worldwide. However, in the current

environment, such capability, as costly as it may be, is a must for such companies. [92] [35]

Another example concerning PayPal, an online payment company now owned by eBay, reiterates not only the common "know who you are doing business with" axiom of the Patriot Act, but also that companies should increase their scrutiny over who they knowingly do business with. PayPal was cited for having violated the Patriot Act by transmitting funds over the past couple of years related to online gambling. EBay has since settled this issue by paying \$10 million in fines and penalties. As indicated above, businesses now more than ever need to extensively research those who they do business with and make educated decisions as to whether to continue the business relationship. This example also relays another salient issue regarding the enforcement of the Act. While the terrorist acts of September 11th, 2001, were quite obviously the impetus of this legislation, the Federal government will also vehemently enforce the Patriot Act towards questionable or illegal activities loosely related or even unrelated to terrorism. [57]

How Companies Become Compliant

From a software engineering perspective, obtaining sufficient background information on people or entities a company may somehow work with presents a significant task to that company. Most companies accomplish this task at least in part by using a list supplied by the Federal government of known terrorists and other criminals. One widely used list is the list of Specially Designated Nationals (SDN List) supplied by the U.S. Treasury Department's Office of Foreign Asset Control (OFAC). Some companies choose to use their own information technology resources to check their transactions against these lists. Others make the decision to outsource this function. The

Patriot Act has initiated a proliferation of private vendors who will work with companies to ensure their compliance (see Section IV of this paper). The following examples describe how a large insurance company achieves Patriot Act compliance through an inhouse solution and how a local credit union does so using an outside vendor.

In-House Solution – Insurance Company

As noted above, insurance companies now fall under the definition of a financial institution as prescribed by the Patriot Act. The large insurance company in this example chose an in-house solution for compliance with the Patriot Act.

This company had a few of its programmers write a batch-processing COBOL application that is run daily to check names against the OFAC SDN list. The names that are checked include any person or business with whom the company will or could have to transact money. Employees are even checked against the list. Any vendor that the company partners with is run against the list as well. Any person or business that the company insures or underwrites must also be checked. Finally, anyone whom the company will need to pay out for a claim, whether insured by the company or not, is checked against the SDN list.

To illustrate, consider one particular programmer charged with the daily reporting aspects of this project. This programmer receives a printout for each match found between the company's list and the SDN list. Nearly every day, there is at least one match, and on some days there are as many as six. The programmer then forwards the information received on the printouts to the legal department for follow-up.

Whether the legal department determines the match to be a false positive or a legitimate match to the name on the SDN list has no bearing on the application. No false

positive information is flagged on the company's list. Such names would continue to generate match reports and would have to be reviewed.

Obviously, the insurance company incurs some measure of cost with this form of compliance, in terms of human, hardware, and software resources. However, this does not represent a significant burden to this particular company. This company has over 200 programmers, most of whom are proficient in COBOL. The time involved for a few of them to write the application initially and for one of them to take on the daily reporting responsibilities is relatively minimal. Also, the company runs hundreds of batch applications using large amounts of storage space and many different files and databases; so the cost to the company for compliance in terms of hardware and software is also insignificant. Overall, the price of this compliance is well worth avoiding the penalties for non-compliance.

[41]

Outsource Solution – Credit Union

The credit union in this example is a small local credit union with two persons and no programmers comprising its Information Technology (IT) department. Therefore, designing an in-house software application for Patriot Act compliance was not a feasible option.

This credit union evaluated a few companies for an outsourced solution before making its choice. The chosen software compares the credit union's list to the SDN list and flags matches, thereby doing for the credit union what the in-house software does for the insurance company.

There was a small amount of legwork involved on the part of the credit union in getting the software up and running. The IT people of the credit union developed a query to write their membership to a file for the new software to use to check against the SDN list, which had to be uploaded to the new system as well. In addition, the IT department had to load the software onto the credit union network and create shortcuts to the software on the applicable desktops. Also, the software cost the credit union under \$1,000 to purchase. In addition to the fact that costs were low with regard to this compliance software, the credit union already was fulfilling many of the requirements of the Patriot Act since it meets the pre-Act definition of a financial institution. Therefore, the credit union has taken on a minimal amount of additional cost due to the Patriot Act. As with the insurance company, the relatively low costs to the credit union of Patriot Act compliance were well worth avoiding the costs of non-compliance.

Feasibility of Compliance

As noted above, essentially any company, whether large or small, no matter what the industry, has likely born some level of information technology cost pertaining to compliance with the Patriot Act. Likewise, many companies incur administrative costs for compliance, most notably the costs of training employees on how to be compliant.

Although nearly all companies do incur some cost for compliance, whether or not the cost is reasonable depends on the type of business in question. As noted above, from an information technology standpoint, the large insurance company and the local credit union were able to attain Patriot Act compliance at a reasonable cost.

The companies which are most likely to have incurred unreasonable information technology costs for Patriot Act compliance are large – national or global - companies

with multiple transaction points that were not considered financial institutions prior to the Patriot Act, such as Western Union. Such a company would have to spend potentially millions to comply with the precedent set in the Western Union case of being responsible for reporting multiple transactions at different locations totaling over \$10,000. Banks have this responsibility as well; but they have had it even before the Patriot Act's inception, so they would likely have incurred such costs before the Patriot Act.

The steps a company such as Western Union would have to take to reach compliance as set by the Western Union case are indeed large in scale. First of all, a company with transaction points around the world probably has had little or no use before the Patriot Act in merging all of its transaction data and thereby being able to determine if a particular customer conducted transactions at several different points. Depending on the degree of management's centralization, it is very possible that different regions or even different individual locations of the company keep their transaction data in different formats, use different file names, use different column headings in their files, etc. Now, with the advent of the Patriot Act, such a company must struggle to find an affordable means by which to pull all of their transactions from around the country or even the world together, convert all records to one single format, and finally check those records against one another for transactions made by the same individual at different locations and/or over different days totaling \$10,000.

In conclusion, Patriot Act compliance seems reasonable for most financial institutions in terms of checking names against OFAC's SDN list. However, for larger companies with multiple transaction points which were not recognized prior to the Patriot Act as financial institutions, compliance with newly-applicable Bank Secrecy Act

requirements of reporting transactions, whether or not from different locations over different days, made by the same individual totaling \$10,000 casts an unreasonable information technological burden on such companies. [48]

As an example of how unreasonable this burden may be, we again refer to Western Union. As noted above, the company fell short of Patriot Act requirements involving transactions totaling over \$10,000. To avoid future fines and scrutiny, all individual transactions aggregating over \$10,000 involving the same person or entity must be reported whether they were sent or received to or from the same location, and whether they were sent during the same day or over multiple days. Currently, Western Union handles over 250 million total transactions (including transfers and money orders) per year among its facilities in over 185 countries. [93] Averaged out over the course of the year, that is nearly 685,000 transactions per day. Doubling this number, to account for the sender and receiver of each transaction, gives us 1,370,000 records to deal with. Also, since any number of transactions at different amounts may aggregate to over \$10,000, none of these records may be precluded from the search due to low dollar amount. Therefore, at a minimum, regarding only one given day, Western Union would need to compare each of the 1,370,000 transactions against one another. This type of comparison, in its simplest form, would require 1,369,999! (factorial of 1,370,000-1) database operations. In and of itself, this type of operation would be an astronomical amount of data processing that would have no business value to Western Union. In addition, other variables need to be considered. First off, as previously noted, Western Union will also need to report on transactions that occur over different days. Obviously, this would greatly increase the already large number of comparisons the database would

need to make. Another variable to consider is whether to enhance the comparisons so that different variations on each name are considered. To be successful, this search would most likely need to consider different orderings of first, last, and middle names; different variations of first names, such as nicknames; and any known aliases of certain individuals. Western Union, to reach complete compliance with the Patriot Act, would have to add data processing capabilities that may not only be unreasonable, but may also exceed the limits of technological feasibility.

Internet Service Providers

The Electronic Communications Privacy Act (ECPA) was passed in the 1960s to give privacy protection to electronic transmissions. It prohibits owners and operators of Internet services from revealing information gathered in the course of business to third parties, and makes it illegal for third parties to intercept transmissions or access stored data. Law enforcement agencies could not access the data either, except under certain conditions. Some sections of the Patriot Act affect the ECPA by broadening the authority of law enforcement officials substantially.

Surveillance

Section 216 of the Patriot Act substantially changed the laws that govern Internet usage which therefore have an impact on Internet Service Providers (ISPs). Under previous law, a government agent can get a pen register or trap and trace order requiring a telephone company to reveal the "numbers dialed" to and from a particular telephone. To obtain the order, the law enforcement agent must simply certify that the information to be obtained is relevant to an ongoing criminal investigation. Under Section 216, a judge must grant the order upon receiving the certification. Section 216 of the Patriot Act

extends this low threshold of proof to Internet communications that are far more revealing than the numbers dialed to or from a telephone, and to portions of email communications that cannot readily be separated from content. Section 216 gives law enforcement agents who obtain pen register and trap and trace orders access to dialing, routing, addressing and signaling information, thus expressly including email and electronic communications. The bill does not clearly define these terms. They appear to apply to law enforcement efforts to determine what websites a person has visited. The "contents" of communications are excluded, but the Patriot Act does not define what "contents" are. This has provoked serious questions about treatment of web "addresses" and other URLs that identify particular content. This extends a low standard of proof to "content" information even while Section 216 purports to exclude content. [2] Does this mean that Internet Service Providers now need to keep their log files of Internet traffic and email longer and if true, how long is feasible to retain these records? At this point it is up to each individual ISP to decide how long it is important to keep records.

Section 216 permits a federal judge or magistrate in one area to issue a pen register or trap-and-trace order that does not name the ISP's upon which it can be served, and that order can be served on ISP's anywhere in the U.S. The judge issues the order and law enforcement agents choose the places at which the order can be served. This marginalizes the role of the judge. Law enforcement obtains the equivalent of a blank warrant. In addition, nationwide searches of pen register and trap-and-trace orders effectively insulate law enforcement from challenge in court. If a small ISP in San Francisco thinks that the FBI is illegally viewing content based on a pen register or trapand-trace court order issued in New York, it would have to muster its resources to fight

the warrant in New York. Given these hurdles, an ISP is unlikely to challenge an overbroad court order, or challenge FBI actions that are inconsistent with the court order. [2]

Carnivore

The tool the FBI uses to perform Internet surveillance is Carnivore. Carnivore gives the FBI access not only to all of the target's communications, but also to the communications of non-targets who use the same Internet Service Provider as does the target. The FBI's solution is for U.S. citizens to trust them because they work for our government. This is entirely unacceptable and possibly in violation of the Fourth Amendment. While Section 216 requires reports on the use of Carnivore, it is not clear as to whom such reports must be sent. The agency that installs Carnivore is required to maintain a record that will be provided to the court, ex parte and under seal within 30 days after termination of the order. When the FBI's use of Carnivore was first revealed in July 2000, there was a great deal of concern expressed by members of Congress, who stated their intent to examine the issues and draft appropriate legislation. To facilitate that process, former Attorney General Reno announced that a Justice Department review panel would check into issues surrounding Carnivore and that its recommendations would be made public. That promised report had not been released when Ms. Reno left office, and Attorney General Ashcroft announced that a high-level Department official would complete the review process. That review, however, was not completed prior to September 11, 2001. As a result of the delay, Congress did not have the benefit of the promised findings and recommendations when it enacted the Patriot Act. Since Carnivore provides the FBI with access to the

communications of all subscribers of a monitored Internet Service Provider and not just those of the court-designated target, it raises substantial privacy issues for millions of law-abiding American citizens.

The new law permits any U.S. attorney or state attorney general to order the installation of the FBI's Carnivore Internet surveillance system, which also has the capacity to capture the contents of email messages. The agency says the public must trust that investigators will not review this information. Unlike trap-and-trace orders, Carnivore requires that investigators set up an audit trail which includes what information was gathered, by whom, and when. It was not clearly specified who oversees this.

Court orders are limited to 30 days, and interceptions must terminate sooner if the objectives are attained. Judges may require periodic reports, to the court typically every 7-10 days, advising it of the progress of the interception effort. The FBI claims these circumstances thus assure close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order, if consistent with requirements of the initial application, are permitted, if justified, for up to a period of 30 days. The Carnivore device works much like commercial packet sniffers and other network diagnostic tools used by ISPs every day, except that it is supposed to provide the FBI with a unique ability to distinguish between communications, that may be lawfully intercepted, and those that may not. For example, if a court order provides for the lawful interception of one type of communication like email, but excludes all other communications like web surfing, the Carnivore tool can be configured to intercept only those email being transmitted either to or from the named subject. At this time it does not work like this. The Electronic Privacy Information Center (EPIC), when it reviewed the

FBI's own documentation, found memos on Carnivore regarding "the improper capture of data." Carnivore attempts to limit the messages viewable by human eyes to those that are strictly included within the court order. ISP knowledge and assistance, as directed by court order, is required to install the device.

The use of the Carnivore system according to the user, the FBI, is subject to intense oversight from internal FBI controls, the U. S. Department of Justice, and by the Court. There are significant penalties for misuse of the tool, including exclusion of evidence, as well as criminal and civil penalties. The FBI insists the system is not susceptible to abuse because it requires expertise to install and operate, with close cooperation with the ISPs. EPIC has multiple examples on its website that contradict the FBI's claims about their expertise at installing and operating Carnivore. Still, what this boils down to is that if the FBI is granted a court order, they can provide the order to an ISP who then has to drop what they are currently working on to assist in the interface of Carnivore to the ISP equipment so the FBI can sniff traffic on the ISP network.

Many ISPs may be unaware of Carnivore and how it can be implemented according to the Patriot Act. Kevin Mitchell from the ISP Iserv states, "We have never gotten any type of court order to let anyone install network monitoring on our network. Carnivore is not welcome in our facility. If such an event took place, we would consult our attorney to see what we are required by law to do. We have worked with law enforcement on investigations where we have received subpoenas or search warrants in regards to user activity. In those cases we do the research and provide the information. Many times we end up having to train the law enforcement people as to what questions

they *should* be asking and what kind of information we need to give them (to make conclusions on) what they're (rationally) looking for."

<u>Client Information an ISP Can Provide to Law Enforcement</u>

The law makes two changes to increase how much information the government may obtain about users from their ISPs or others who handle or store their online communications like employers that provide Internet access or email to employees.

First, section 212 allows ISPs to disclose the content of stored email messages and other customer information to law enforcement with no need for any court order or subpoena, if the provider "reasonably believes that an emergency involving the immediate danger of death or serious physical injury" justifies disclosure of the information. This means if an ISP is monitoring its users for business purposes it can turn over anything that it thinks is unusual without reprieve.

Second, sections 210 & 211 expand the records that the government may seek with a simple subpoena to include records of session times and durations, temporarily assigned network IP addresses and means and source of payments, including credit card or bank account numbers. The exception allows disclosure of these customer records (1) with the consent of the customer or subscriber, (2) when it is necessary to the rendition of the service or to protect the rights or property of the service provider; (3) to a governmental entity when the provider reasonably believes that an emergency involving immediate danger of death or serious injury to any person justifies disclosure of the information, or (4) to any person other than a governmental entity. The above permitted disclosures have privacy and security considerations for employers because information

that is generally considered proprietary or confidential by an employer may be accessed or disclosed by an Internet Service Provider. [55] This has caused many ISPs to purge traffic records such as websites visited, session times, assigned IP addresses on a short time table so that if their records are subpoenaed they only have a few days' worth of records to provide. Plus, traffic data takes up large volumes of disk space so it is not feasible to keep the various log records for large amounts of time. Kevin Mitchell who is in charge of any Search Warrants issued to Iserv ISP said "There is no mandate (that I've been made aware of) as to how long we need to keep logs. How long we keep logs for particular servers or services depends largely on hard drive space and how critical keeping these logs is to our business. For example, Iserv will keep two months worth of web site logs (the current and previous month), but we'll keep a year worth of dialup usage. Email logs we keep approximately three months or so."

Section 211 also amended Title III to stipulate that where a cable company provides telephone or Internet services, it must comply with the laws governing interception and disclosure of communications by other telephone companies or ISPs. The new law supercedes the original provisions of the Cable Act relating to obligatory and voluntary disclosure of subscriber information, although the amendment would provide an exemption for "customer cable television viewing activity." However, the stringent privacy protections prohibiting release of customer information to nongovernmental entities without the customer consent remain in place.

<u>Clarity of Expectations</u>

Another concern for ISPs is that the hasty passage of The Patriot Act made an already murky situation even less clear. Some say it is now more difficult for technical
personnel to know what they should hand to the government and what they should keep to protect their customers' privacy. Civil libertarians are concerned that officers might have been given too much leeway. "The Patriot Act leaves standards up in the air for engineers and people who run ISPs," said Ari Schwartz, associate director for the Center for Democracy and Technology in Washington, D.C. "It's difficult for people (ISPs) to know what to do if the government wants information; they're not sure what to turn over and what to keep. The law is written very vaguely. The problem is how to stop the rogue actor." There's also concern that when the government tells ISPs and others exactly what to keep, this will stifle creativity while providing known guidelines that criminals might find simpler to exploit. "We're for standards, for setting rules about what is content so that people have an idea what to get and what to keep," Schwartz said. "But we're against design mandates, telling innovative engineers how they have to build systems. If terrorists know the systems only store information for 90 days, why not wait 91 days before they act? Specific mandates can make it easier for them to work around." [23]

IV. Opportunity/Growth Impacts to Business

Overview of Businesses

Many businesses are taking advantage of the new mandates passed down by the Patriot Act and providing Software, Data Analysis, and Security services to help companies in various industries cope with the more stringent regulations. The challenge of complying with the mandates largely lies in an organization's ability to connect and secure their mix of disparate systems that often span widespread business units. Noncompliance with these standards can lead to a damaged reputation within the industry, paying heavy fines, and even imprisonment. As more and more organizations struggle to

meet these regulatory mandates, many are turning to software solutions that help support their compliance efforts. Some feel that technology is key to compliance. Given the evolving nature of some of the mandates, it is worthwhile to choose a solution that is flexible and extensible to accommodate the regulations' future amendments and changes.

There are numerous companies with various ranges of software experience entering this arena. Celent, a research firm, recently came out with a listing of the top Transaction Monitoring and Watch List Monitoring companies. These companies vary in their means to assist diverse businesses to meet the compliance of the Patriot Act. Businesses had an October 2003 deadline to go through their present procedures to meet the requirements of the Patriot Act. Most of them decided to add a technology solution that will provide a means to run their database against the government's listing of potential terrorists. With a steep fine for not finding a way to meet the Patriot Act, every one was scrambling to find a software vendor that will interface not only with their core systems but also will meet all of the facets of their industry that are affected by the Patriot Act. It is important for all industries affected to take a look at the entire realm of connectivity with vendors to realize all aspects and databases that need to be run against the list prior to seeking a Patriot Act vendor. One example of this is Wisconsin University. They have two databases that store information about foreign students. In order to run against the list, they have to combine the two into one database and then transmit it to the government. They had to select a vendor that allowed data integration in the software solution. [16]

Software solutions vary in cost and purpose. The stand-alone systems, that require more manual intervention, are less expensive than the ones that integrate with core systems. Some software focuses on transaction monitoring, and others focus on comparing company databases to the Federal List. Due to yearly licensing and maintenance agreements, the opportunities are still ripe for vendors to take a piece of this market. Depending on the research done, the actual cost estimates vary, but according to Celent, companies will spend \$632 million on software, hardware and other services in the next three years. [14] An article in Computerworld.com states, "...the U.S. brokerage industry will spend as much as \$700 million through 2005 on technology and outsourcing services in order to comply with the antiterrorism and anti-money-laundering regulations of the USA Patriot Act." [66] There are other companies that will benefit from the Patriot Act.

"According to TowerGroup, about 39% of compliance budgets is being spent on integrating back-end systems, and 35% is going toward new software. Another 24% of the money is being used to upgrade IT infrastructures, such as hardware and storage, the report states. The remaining 2 % is paying for outsourcing services with operators of customer databases, such as Regulatory DataCorp International LLC (RDC) in New York."[66]

It becomes clear that not only software vendors are capitalizing on the Patriot Act, but also consulting firms and hardware vendors. However, software vendors alone are seeing a strong increase in their business due to the Patriot Act, some as much as 200 percent or more. [61]

	Transaction Monitoring		Watch List Filtering	
Rank	Large	Small-Medium	Large	Small-Medium
	Institutions	Institutions	Institutions	Institutions
1	Searchspace	Actimize	FircoSoft	Prime Associates
2	Mantas	STB Systems		Americas Software

3	ACI Worldwide	Prime Associates		Bridger Systems		
Vendor to Watch	SAS Institute	Infrasoft				
Source: Celent Communications						

Software developers take unique development techniques to draw customers:

- Behavior Detection
- Use of scenarios
- Comparing databases off site against the Federal Database
- Some work with multiple platforms
- Most vary in the different ways that the comparisons are made to the Federal Database. Some compare just with the name of the terrorist, others compare several different fields.
- Integrations into core systems
- Stand alone systems that are inexpensive but require manual intervention

As the listing indicates, there are many selections available to the user. By making a call

to any one of the vendors and indicating the individual needs, a fit can be made.

When looking for a software vendor, certain software requirements top the requested

list from businesses:

- Matches on a variety of criteria
- Automatic updates to the OFAC file as it is available
- Accurate and quick results
- Integration with the core software system(s) used
- Supportive of an organization's specific policies and procedures
- Scalable to an increase of customer base
- Adapting to new regulations as needed
- Easy upgrades
- Ability to eliminate false positives
- Pull and store reports

• Cost effective for the organization

Companies

<u>Mantas</u>

One company that claims to meet most of these requirements is Mantas. It is number two on the Celent Communications research chart for transaction monitoring. They have more than 15 years of experience in the financial industry. It can process up to 325,000,000 records per day or up to 10,000 instances per second. This may not be important for smaller businesses, but it is essential for larger institutions. Their packages are entitled Enterprise Integrity Suite and Enterprise Opportunity Suite. They both look for transactions but at different angles. Relationships and behaviors that other software may miss, they claim to find. As data is entered, it is run against scenarios that have been created by specialists in the field. These scenarios change as business needs change. Lastly, they create an audit trail to prove to any Federal Agent or Regulator that as an organization due diligence is occurring. The selection of this software vendor pledges a proprietary detection technique. Mantas is rare in that it uses scenarios for behavior detection.

Behavior detection is the ability to look through data to "identify suspicious events and related entities over time, separate them from normal everyday events, and then to zero in on the perpetrators." Mantas believe that without their software piece using this technology, behavior can go undetected for years. Financial services are currently using five different levels of compliance software to look for suspicious transactions. Level Zero is manual investigation. This is labor intensive for staff. Level One is looking at

each piece of data separately. Level Two is using simple procedures to find fraud. Level Three is looking at "subsets" to determine theft. Mantas uses Level Four Technology that detects the hard to find abuses of illegal activities. They reveal how a thief may attempt to do business with transactions or events. Most will not do the transaction under the same name nor will they do the same transaction twice at close times. That is what Mantas claims to do best: they look at the relationships between the data and zero in on potential fraud. To find these relationships they use Link Analysis and Sequence Matching. Link Analysis is finding commonalities between the data or what links them together like a similar address or a phone number. They also use Sequence Matching, which looks at behaviors over a short period of time such as sudden movement of funds. [64] It appears, at least for one of Mantas clients, that their software purchase has paid off. As the Mantas reports came in, there were small companies doing business with them and on the surface looked legitimate, but were not. It was turned over to law enforcers for prosecution. [25]

CAPPS II

The aviation system is also looking for Patriot Act solutions. They have begun the development of CAPPS II or Computer Assisted Passenger Prescreening System II. The Transportation Security Administration, or TSA, is financing this automatic screening system. There are two companies assisting in the development, Lockheed Martin Management and Data Systems. Lockheed Martin was awarded a 5-year contract with the first phase costing TSA 12.8 million dollars. [10] When entering an airport, the system would have connections to public and private databases and would flag some people to

enter the terminals and others to be pulled to the side for questioning. The program is written to determine the risk assessment to assist in aviation security.

There have been numerous concerns about privacy since the passenger information, which includes passengers providing not only their name but also their addresses, phone numbers and dates of birth. That data is then run against other databases. A result of green, yellow or red is then shown to the aviation employee. The result will not include the FICA score, which is shown on an individual's credit report, as well as any other private data. In fact, the data will be destroyed within a set amount of days after the flight itinerary is completed for U.S. citizens. This was not the way it was originally planned. Due to public outcry, TSA has altered this program to ensure privacy of U.S. citizens. The system is currently under testing with Delta Airlines.

Already people have been pulled to the side at airport terminals, with armed guards at their sides while their backgrounds are being checked and the FBI is being called in. A student at Columbia University claimed that the attendant at the ticket counter gave him a "bewildered look" and then the guards were called in. Another English teacher indicated that he felt good knowing that they were doing additional screening on him. He told the reporter, "These [the terrorists] are not people that you want to fly with." Another flyer stated that it took months to get his name off the list and indicated that TSA needed to get a better procedure for people to know how to clean their names from the list. The student at Columbia indicated that he had found a loophole to the software already. "If I go by my first initial, middle name, and last name, there is no problem." But there is. If he has found a way, so will the terrorists. [1] This indicates that the CAPPS II system is only as

accurate as the program that runs it against the Federal Database or the data contained there in.

It is still undetermined how long the CAPPS II database will store foreign visitor data. In an article in the *Washington Post*, two Pakistani men were attempting to purchase airline tickets. An employee ran their name against the "no-fly" list, and they came up as a positive match. The authorities were called in, and positive match was confirmed. [44] This causes U.S. Citizens to feel better about the effectiveness of the CAPPS II system. However, it also indicates that other foreign people whose names match the listing also have been detained for no reason. TSA has set up procedures for those people to contest or amend records, but they must send in a written request. One thing becomes clear: non-U.S. Citizens are not protected by our Privacy Rights. CAPPS II is expected to be implemented in 2004. [100]

As the code is being developed and revised as changes are made, there are already plans to expand the databases that will be accessed as plane tickets are purchased. It will be searching Federal and State databases for anyone with outstanding warrants. Another database that will be accessed is the US-VISIT or U.S. Visitor and Immigrant Status Indicator Technology program so that entrance and exits into the U.S are kept consistent. TSA claims that all of this will be coded with respect to the Privacy Act of 1974. [100] According to the Privacy Act, any U.S. citizen has the right to see what the government has in their databases about themselves. [34] However, one of the aspects of the Patriot Act is that a match is kept secretive until the Government takes action. Many feel that the Patriot Act itself is in violation of the Privacy Act.

<u>CRM Solutions - Searchspace</u>

Other companies are using their existing CRM software. Customer relationship management software allows companies to know whom they are doing business with and to track their behavior. This allows them to serve the customer base more efficiently and to know which of their products are doing well and which products may need enhancements. Many organizations have already invested in this software that Oracle, Searchspace, and many others developed years ago. Consequently, they have grown to know their customers' ways before the Patriot Act was designed. Searchspace claims to have an integrated software piece that works with the existing CRM solution. There are many companies that claim that they can pull the data out of the CRM solution to analyze fraudulent behavior. Using this strategy will let them know not only who may match the Federal database but also who their good and not-so-good customers are. [25]

Compliance

One item that seems to appear in most of the marketing campaigns for these companies is the promise of compliance. As this paper discusses, the Patriot Act is vague regarding compliancy. The best rule-of-thumb for an organization is to know with whom they are doing business and assuring due diligence in checking identification. Software alone cannot ensure compliance. And, more importantly, until all databases are interconnected, can true compliance to the Patriot Act be accomplished? [88] Also, individual businesses have their own policies and procedures with respect to the Patriot. What one business does to rectify compliance may differ in another business. Even the Mantas software has taken the Patriot Act to a higher level than most. There are the minimum requirements, and then there are the software vendors that are looking into the future to meet any additional needs. It is possible to be in compliance without the

assistance of software for extremely small businesses. However, to ensure that compliance is being met, software is definitely a must.

Citigroup is one company that is temporarily taking a "Low-Tech" solution to the Patriot Act. They have 200 million accounts that need to be run against the Federal database. Given the size of their system, and the fact that they only have one address field, they are turning to pen and paper. When the new system is installed, all the data will need to be input. They say it may be as long as next year. So for businesses with their own programmers and solutions, outside vendors will not be considered. They will attempt to develop their own software in a fast track mode. [62]

Foreign Country Needs - Sybase

Software companies realize the impact that the Patriot Act has on foreign companies and banks. Some believe that the majority of the software sales will not come from within the U.S. but from foreign companies that want to do business with the U.S. [105] This is an opportunity to develop software for a group of individuals who want to continue to do business with U.S. companies, and to do so, they need to meet the Patriot Act's criteria. The Patriot Act indicates that U.S. banks have to do due diligence when doing business with non-U.S. banks since their relationship allows them access into the U.S. monetary system. It also indicates that U.S. security firms and banks cannot do business with shell banks, those foreign banks that do not have a physical presence and have no affiliation with another bank. The Patriot Act goes further to say that if a foreign bank is doing business with a shell bank, the U.S. bank can not do business with that foreign bank since they have an indirect relationship with a shell bank. If a U.S. Bank does conduct business with a foreign entity, whether person or bank, the U.S. government

has the right to obtain that information. If the information gathered is linked to terrorist activity, the U.S. government has the right to seize such assets. As this indicates, the Patriot Act has considerable impact on non-U.S. people and businesses. [96]

Sybase is one such company that is doing well in the foreign market. They recently signed up the People's Bank of China. For foreign banks and firms, it is advantageous to purchase a software solution with a U.S. Company since they are already selling to the U.S. market. On a side note, however, there is a recent controversy surrounding the Sybase Company and President Bush's brother. It seems that Marvin Bush, George W. Bush's younger brother, works for Winston Partner that has 5.5 million shares in Sybase. One article states, "Business for Sybase is business for Bush, and the Patriot Act boosted business." [11]

Consulting

As the Patriot Act was introduced, businesses of all types panicked. As new regulations and requirements are introduced into law, having a Compliance Officer assists the organizations in providing direction to obtain compliance. Even then, there were many educational conferences offered. Many businesses attended more than one conference since different people were interpreting the Patriot Act in different ways. Some businesses, such as libraries, were mystified by the Patriot Act. This confusion promoted the entrance of consultants to offer their expertise. Consultants are used for varied reasons, from as simple as defining the Patriot Act to going as far as finding a company that will fit their core software and integrating it with their own. Training is also needed in order to run the software to its fullest extent and to understand the reports and daily duties. Even though a company may not have an in-house Compliance Officer,

they may have IT staff that will be called upon to provide the direction needed. However, more than 75% of IT managers in an article in *Computerworld* indicated that they, or their departments, do not have Project Management training. [46] The article indicated that consulting firms expect to see an increase in Project Management training due to the Patriot Act just like it occurred during the Year 2000 for the Y2K bug. One such company offering its services is STB Systems. They offer scoping, design and analysis, project management, training, and finally, installation and implementation. For those businesses such as libraries that do not have technical people on staff, STB is a likely vendor candidate.

Data Mining

The government policy implications associated with the Patriot Act center on three primary issues: knowledge management, information security, and privacy. Knowledge management has been defined as "the process through which an enterprise uses its collective intelligence to accomplish its strategic objectives." [13] Enhanced data sharing and knowledge management techniques are expected to play a significant role in homeland security efforts. Several of the provisions focus on improving access to and the sharing of centralized databases by federal, state, and local law enforcement agencies. Some of the provisions also seek to establish a more fully integrated database system for processing and tracking the granting of visas, as well as the entry and exit of foreign nationals in the United States. In many cases, these provisions are designed to rectify the problems associated with having multiple, incompatible, and sometimes overlapping databases, which have been identified as one of the contributing factors to the difficulties law enforcement and intelligence agencies have had tracking suspected terrorists. [13]

Knowledge management has been recognized as an important component of improved homeland security. Knowledge management efforts involving government have so far encountered a variety of obstacles. Some of these obstacles include creating the appropriate technical and support infrastructure, achieving user "buy-in," and managing the development and use of specialized information created by data mining. Some have suggested the creation of the position of chief knowledge officers (CKO) at the agency, department, and federal level to facilitate the execution of specific knowledge-intensive projects and support larger government reform efforts. The success of knowledge-management efforts in the homeland security area could affect the adoption of many sections of the Patriot Act.

Information security is another potential large obstacle to the public. It is assumed the data is secure, encrypted, and accessed only by specific authorized users. The issue is: who are those users that have access? And, who ensures that they do not abuse their privileges?

Finally, the implications of the Patriot Act on privacy could have a negative effect on government initiatives. The sentiment is that the loss of privacy as a result of government is a significant concern among citizens. The Patriot Act greatly expands the type of information that may be collected by law enforcement officials. Concerns about potential misuse of data mining provisions could dampen citizen enthusiasm for carrying out electronic transactions with the government. [24]

Data Mining is the use of methods to uncover patterns in data. Profiling is the recording and classification of behaviors. This occurs through aggregating information from online and offline purchase data, supermarket savings cards,

white pages, surveys, sweepstakes and contest entries, financial records, property records, U.S. Census records, motor vehicle data, automatic number information, credit card transactions, phone records, credit records, product warranty cards, the sale of magazine and catalog subscriptions, and public records. Companies collect information derived from a number of resources to build comprehensive profiles on individuals in order to sell products and to sell dossiers on behavior. This is often done without notice or extending a choice to the individual to opt-out of the dossier building. Marketers for target advertising may use these dossiers, and they may be sold to government for law enforcement purposes. [31] For the purpose of the Patriot Act, data mining involves maintaining a large database on individuals that draws its information from private and public databases. When applying it to the Patriot Act, it is using computer data to uncover patterns that may fit illegal activity without basing it on individual suspicions. [59] Some of the records that would be accessed are credit reports, medical records, and most any data stored in any database.

Senator Feingold is an advocate against data mining. He feels that there needs to be congressional oversight and review of this data in order to ensure the privacy rights of Americans. The Privacy Act of 1974 was enacted to do just that. According to the Act, any U.S. citizen has the right to see what the government has in their databases about them. [34] However, with the Patriot Act, the government has put a gag order on any business that reports a potential terrorist, and they do not need to inform the citizen. Thus, individual citizens may not ever know that the government has accessed their data, and they probably would not

know the government even has records about them much less if the records are accurate or not.

Section 361 of the Patriot Act establishes the Financial Crimes Enforcement Network (FinCEN) in statute, and charges the bureau with establishing a financial crimes communication center to facilitate the sharing of information with law enforcement agencies. FinCen is also to maintain a government wide data access service from information collected under the anti money laundering reporting laws, information that includes national and international currency flows, as well as information from federal, state, local, and foreign agencies and other public and private sources. [24] Section 414 expresses the sense of the Congress that the Attorney General, in consultation with the Secretary of State, should fully implement the entry/exit system as expeditiously as practicable. Particular focus should be given to the utilization of biometric technology and the development of tamper-resistant documents. Section 701 also calls for the Department of Justice establishment of a secure information sharing system. It does not stipulate if it should be the government doing the work to make the data secure or whether it should be outsourced to a private company to guarantee data security and who has access to the data

Hidden in the small print of individual's doctor's privacy statement, there is a line that grants the government the right to look through your medical records. [3] The government now has the right under Section 503 of the Patriot Act to add "any crime of violence" offenders to their DNA database. Is it not feasible this database could be mined against biometric data accumulated in Section 414 for entry and exit into to the United States? This is meant for collecting data on terrorists and potential terrorists, but if taken

one step further, the government could start looking for patterns in the DNA of terrorists and then compare it to DNA in private medical records to look for people who may be more predisposed to becoming terrorists because of their DNA make up.

The 1974 Privacy Act fails to cover contractors who provide the government with access to the databases that they already operate for their own purposes. Indeed, regulations issued in 1983 reinforced this point by requiring contractors to be subject to Privacy Act compliance only when "the design, development, or operation of a system of records on individuals is required to accomplish an agency function." [59] Thus, the Privacy Act fails to cover those times when the agents in the federal government decide they would like to take a peek at already existing private-sector databases that may be of interest. A private company can create its own database, and then using profiles and data mining, do its own terrorist investigation, providing the information to the government on its own accord. The private company and the government agency it provided the information to would be the only two parties privy to how this information evolved. This indicates that there is potential for the FBI to be manipulated from the private sector under the guise of public welfare. Private companies already perform such a service.

There are federal and state legal restrictions that prevent the government from building dossiers on individuals without cause. However, these protections do not prevent the private sector from building comprehensive profiles on individuals. The government can then purchase this information from the private sector. Several companies, including Experian and ChoicePoint, possess multi-million dollar contracts with the federal government to sell personal information to law enforcement. Profiling partnerships

generally rely on the compilation of public records and are covered in more detail on the <u>EPIC Public Records and Privacy Web Page</u>. [31]

A number of commercial profilers sell public records information to government law enforcement agencies. An April 13, 2001, article in the *Wall Street Journal* reported that profiling company ChoicePoint provided personal information to at least thirty-five government agencies. To date, EPIC has determined that ChoicePoint has several multimillion dollar contracts with law enforcement agencies to sell personal data. In addition, Experian, a credit-reporting agency, sells personal information to government agencies for law-enforcement purposes. [31]

Another loophole used to get private records into government databases occurs when Defense Advanced Research Projects Agency (DARPA) does research that is performed by contractors who can acquire public database's records for incorporation into DARPA's database. Since DARPA's database is government database, it is accessible by any other government agency.

Private companies could easily serve their own interests or be fooled into serving the interests of others. This would pose problems for individuals who get turned in as fitting a certain profile criteria when data mining is performed. It is very easy to get caught up in speculating what could happen by taking advantage of loopholes in the law and handling data that could affect individuals.

Some people feel that inaccurate data mining profiles may have already impacted our entire country during the 2000 presidential election. The botched Florida felon purges in the 2000 election year left some legitimate voters unable to vote. The numbers fell disproportionately on black Floridians and, by extension, on the Democratic Party,

which won the votes of 9 out of every 10 African American voters, according to exit polls. [79] Early in the year, the company, ChoicePoint, gave Florida officials a list with the names of 8,000 ex-felons to "scrub" from their list of voters. Ironically, none on the list were guilty of felonies, only misdemeanors. The company acknowledged the error and blamed it on the original source of the list -- the state of Texas. [74]

Furthermore, when information is obtained by a government agency, if it is involved in law enforcement or intelligence, they are not required to maintain either accurate records or even to let individuals have access to their records and to correct inaccuracies. Information that makes its way into the "system" operated by federal law enforcement do not have to apply the safeguards of the Privacy Act. Plus, federal law enforcement agencies can pass that information on to other requesting agencies for lawenforcement purposes at any level of government. [59] Now if the FBI conducted data mining with a hypothetical profile and an individual's name came up, this could have traumatic impact on the individual's life, e.g., the U.S. citizens not being allowed to vote in Florida. Suppose that in the course of the investigation (which they can do per Section 507 of the Patriot Act), the FBI obtained the college records of an individual by court order. The individual is never charged and never knows of the investigation resulting from the data mining. Then, the individual and another person are up for a state grant, and the issuer checks the FBI database and finds out the individual had been investigated - though not charged. This fact could make the other person a safer choice to receive the grant, thus biasing the outcome. With the FBI inventing hypothetical profiles and with data mining, something of this nature is probable.

In January 2002, a New York jury awarded \$450,000 in damages to an individual who lost a job opportunity because his profile contained a false criminal conviction. In that case, the judge found that ChoicePoint either intentionally maintained substandard procedures for verifying accuracy of data or should have known that its procedures were substandard under the Fair Credit Reporting Act. In May 2002, FBI agents Lynn Wingate and Jeffrey Royer were indicted on fraud charges relating to use of government databases. The FBI agents allegedly used their access to agency databases to provide information on companies for stock manipulation purposes. One agent allegedly searched the NCIC database and used information contained within it to smear a company executive and lower stock prices. Both allegedly used confidential FBI databases to monitor government investigations of the other stock manipulators.

In April 2002, private-sector profilers met to discuss how they could compile consumer information for terrorist risk profiling and sell it to the government. That meeting, organized by the Center for Information Policy Leadership (CIPL), was attended by a number of companies that are attempting to sell their marketing products for anti-terrorism purposes. [31]

Government can use public records in order to discriminate against certain populations. For instance, during World War II, census records were used to facilitate the internment of Japanese Americans. [31] What is alarming is the government compels citizens to divulge certain information before participating in democratic processes. For instance, for purposes of voting registration, each citizen must verify his or her identity and address. Some districts also collect

information on party affiliation. If a citizen donates over \$200 to a candidate or political party, the citizen must provide name, address, and employment information under federal fundraising rules. This information is often in the public record and may not be protected by use limitations or other Fair Information Practices. This personal information often is used to build complex profiles of citizens and their likely voting behaviors. Aristotle, a company that creates voterprofiling software, sells databases of voter information that includes name, address, phone number, donation history, and party affiliation. The company also sells tools to track voter correspondence with elected officials. [31]

Many people are misinformed and believe profiling is illegal. Profiling is legal. Here is a good example. In a drug case, a detective at the Kansas City Airport said his attention was drawn to a passenger from Los Angeles because he was a "roughly dressed young black male." The detective said he knew that Los Angeles gang members were often drug traffickers who brought cocaine to Kansas City. The man was arrested and convicted. He appealed. The appeals court acknowledged that an arrest based solely on race would be improper. But it said the detective had information beyond the fact of the suspect's race, namely that young members of black gangs were bringing cocaine to the area. That court affirmed the conviction and, in essence, racial profiling itself. "Facts are not to be ignored," the ruling said, "simply because they may be unpleasant." [40]

Casinos are the biggest users of consumer profiling in any industry. In addition to traditional consumer profiling based on purchases and club membership cards, casinos use facial recognition and other technologies to

identify customers. One casino reportedly has a full terabyte of personal information on its customers.

Under Section 215 of the Patriot Act, the FBI can access individuals bookborrowing records from the public library. They can do this without having to specify what they are investigating. They also use the power granted them under Section 215 to review the records of a travel agency. Plus, due to the existing laws requiring reporting of the purchase of guns, they have a list of more names. The examples go on and on, and the collected data accumulates in law enforcement databanks ready to be data mined. Whether or not the powers of the federal government to mine data make us safer from terrorism is debatable. The government has yet to prove its efficacy in fighting terrorism. Citizens have every reason not to feel comfortable about the information that the government's law enforcement and intelligence agencies can obtain about them, place into their databases, engage in mixing and matching of individual's records, and share that data with other government law enforcement and intelligence agencies.

The boundaries between public and private data are not clearly defined. It is easy to see how innocent citizens can have their information in private databases mined and the wrong conclusions drawn, resulting in misfortune. Once the wrong information is in the system, it will not be easy to have it corrected. In fact, the odds are suspected individuals will never know that they are being investigated. Loopholes can allow private information on individuals to suddenly become the government's. As U.S. citizens, we do not know what precise information the law enforcement and intelligence and national security agencies are gathering now or plan to gather in the near future. Without the checks and balances, how will it be known that the most competent people are creating

and maintaining the database and performing the data mining for the government? The Patriot Act is a curtain that is concealing from the public the actual mechanics of the data mining and profiling being used because it is now part of the war on terrorism and linked to our national security.

Another side effect of the Patriot Act is that the federal government is enlisting American universities to assist in maintaining surveillance of foreign students residing in the United States. The Student and Exchange Visitor Program (SEVIS), launched February 15, 2003, will involve almost 6,000 U.S. colleges and universities in gathering and forwarding information about foreign students to a national computer database. Along with other information gathered, the schools must notify the Immigration and Naturalization Service (INS) if a foreign student fails to enroll or is arrested. Institutions that do not have INS approval to participate in the data gathering system will be prohibited from enrolling new foreign students. On March 1, 2003, the INS was merged into the new Department of Homeland Security and is now the Bureau of Citizenship and Immigration Services. [22] Creating comprehensive homeland security will cost trillions of dollars and completely change the way Americans lead their lives. As in George Orwell's 1984, it would include national identity cards, surveillance, public searches, random searches of vehicles, compiling dossiers on all persons who fit specific data mining profiles, tracking the comings and goings of subway riders electronically, putting Global Positioning Systems in all cell phones, and the list of Big Brother programs goes on and on. Virtually everything anyone does, 24 hours a day, would be subject to constant monitoring for anything deemed out of the ordinary - when the data gets mined against the determined profiles. A main concern of the general public is not knowing

what the government's determined profiles are, who creates these profiles, and who is in charge of making sure they do not violate the rights of U.S. citizens. Under the Patriot Act, this information does not need to be shared with the public.

The Patriot Act allows the sharing of data, but it is the Homeland Security Act signed by President Bush on November 25, 2002, that created the new Department of Homeland Security (DHS) and granted it momentous responsibilities and powers to uphold the Patriot Act. The DHS will provide coordination to government anti-terrorism efforts. The new Department will have wide-ranging authority to compile, analyze, and mine the personal information of Americans. The Patriot Act itself includes no new authority to collect information because that power was granted with the Patriot Act. Important issues of oversight and control remain to be addressed. The DHS consolidated 22 government agencies, including the Coast Guard and Secret Service, into one agency. The new Department is tasked to access, receive, and analyze a wide array of information that includes law enforcement information, intelligence information, and other information from agencies of the Federal Government, state and local government agencies, and private sector entities and can enter into cooperative agreements to obtain such information, covering a wide range of contractual or mutual sharing arrangements. Except as otherwise directed by the President, the Department shall have access to unevaluated intelligence. The DHS is expressly authorized to receive wiretap information and grand jury information collected by any other agency. DHS can accept paid or unpaid staff analysts from the private sector, which means that corporate employees could have access to all information available to the DHS. [13] If the Patriot Act is considered to be vague and confusing, the Homeland Security Act is worse.

In May, Attorney General Ashcroft loosened long-standing FBI investigative guidelines to lift restrictions on FBI surveillance and data mining activities, even when no criminal activity is suspected. Both of these initiatives diminish privacy and potentially chill political speech. In both cases, Congress has not established effective mechanisms for oversight. As a result, a great deal of activity that could reduce American's privacy has been conducted behind closed doors. [13] A spokesman for the new Transportation Security Administration has acknowledged that the government has a list of about 1,000 people who are deemed "threats to aviation" and not allowed on airplanes under any circumstances. And in an interview with Salon, the official suggested that political activists might be on a separate list that subjects them to strict scrutiny but allows them to fly. [60] This would account for the growing number of complaints that certain individuals are always being stopped and searched at airport checkpoints.

Essentially, the money laundering legislation of the Patriot Act has led to the obligation of private companies doing data mining in search of potential suspicious activity. They then report it to the government. The costs of collecting and providing information to the government can be burdensome. In industries like banking and communications, where the government makes frequent demands for information, companies must often establish a department that has the sole purpose of processing and responding to government requests. The large telephone and Internet service providers, for example, have entire staffs of clerks, attorneys, and former law enforcement agents, which often number 30-50 employees, just to handle government subpoenas and court orders. [65] The government usually has reimbursement provisions that entitle private business to

compensation for its cost in assisting the government. For example, the Electronic Communications Privacy Act provides that the government must compensate a telephone company or Internet service provider for its expenses, with a court determining what is a reasonable amount if the government and the company are unable to come to an agreement. [65]

SAS Institute, Sybase, and Mantas are companies that already have datamining tools that will identify abnormal transactions to help with compliance in the financial industries. SAS entered the anti-money-laundering software market last year with data-gathering and reporting software that lets customers modify and prioritize the logic that determines what data gets collected and how it is assessed. The software refines business rules and formulates new ones to increase the accuracy of its automatic detection engine. Analytics help weigh rules violations and rank suspicious behavior. Using one system to analyze customer transactions across all parts of a business is essential as criminals find ways around new rules. Mantas Corp.'s anti-money-laundering system runs on Sun's computers and performs link analysis, examining all transactions for suspicious behavior. Vendors are now picking up on ways to turn the compliance effort into business opportunities. Ten-year-old Searchspace Corp.'s transaction-monitoring system has an application to identify possible money-laundering activity. But other applications address business needs, such as detecting fraud and monitoring sales practices. For example, a brokerage firm could use the system to monitor for internal abuses such as insider trading or to track brokers' sales performance. "If you have a solution that can look at every transaction across the organization, can

understand the behavior of every customer transaction on every product in real time, then why would you only use that platform for money-laundering detection?" says Searchspace CEO Konrad Feldman. Searchspace clients use the system to identify any bad-apple customers. Eventually, Feldman believes businesses will "leverage this infrastructure purchase to better understand good customers." Searchspace claims it can be integrated with any existing system, so it can exploit underlying analytics in order to make better decisions.

The use of data mining along with profiling is legal. However, as shown there are many ethical concerns that need to be addressed. The main concern seems to be the assurance that the fox is not guarding the hen house. With the U.S. government's past flawed record of full disclosure to the public, it is hard to be certain that the Patriot Act has not granted powers to individuals who will profile U.S. citizens and data mine on those profiles to manipulate our current systems to achieve goals that are beneficial to the few and harmful to many.

V. Government Impact

The overall impact to all levels of government is one of extensive crosscommunication from one level of government to another and across government agencies within the same level of government. This includes greater cooperative work efforts and communications. Training on new processes and impacts is being completed as joint sessions - including all levels of law enforcement and agencies. Creating better communication across agencies within levels of government, particularly the Federal level, is occurring by joining together information so the greater governmental

community can utilize it. In general, all these items point to a more unified front against terror and foreign crimes against our country and our citizens.

Local, County, State Government/Agencies

Most local, county and state agencies have been impacted by increasing communication among their own units about the Patriot Act and its possible implications to their functions. The agencies at these levels most involved in specifics of the Patriot Act would be in the area of law enforcement. Communications and coordination with the Federal Agencies requiring information based on investigations and handling of detainees would probably be at the top of the list. Many of the federal government agencies involved in rolling out new regulations and/or procedures have significant communication and task force creations crossing levels of government. Training sessions and task force meetings discussing the new regulations and the implications at the state, county and local level are occurring across the United States.

A specific issue relates to county jails. The USDOJ (Department of Justice) – Office of Inspector General (OIG) reviewed a case where detainees held for the federal government in a county jail alleged Section 1001 violations. Allegations included that detainee protest resulted in detainees being beaten by correctional officers. The OIG also reviewed treatment of aliens detained in county facilities in the months after September 11, 2001. "The review included processing, bond decisions, timing of removal from the United States or their release from custody, their access to counsel, and their conditions of confinement." Upon completion of the review, the OIG recommended changes to the FBI on defining consistent standards for handling of detainees. Any new

standards would impact processes at local and county jails that house federal detainees. [85]

An additional specific area of implementation includes impacts to public libraries. Multhomah County Library, like many public libraries across the country, is concerned with communicating to the public its position on the Patriot Act, and those implications to its users. They are concerned with providing services and cooperating with law enforcement, but yet being aware of the constitutional rights and privacy rights of its users. The debate with libraries concerns the information that can be subpoended as part of a court case or investigation. Multhomah's opinion is that the information they keep on file relates only to current check out or past due books and information, and any history is not kept for any period of time. The policy based on the Patriot Act really doesn't change from the prior regulations. "The American Library Association Council adopted a resolution stating the 'sections of the Patriot Act are a present danger to constitutional rights and privacy rights of library users'." Multnomah County Library's website also referenced some legislation underway to exempt library and bookstore records from certain parts of the Patriot Act. From this information it appears most public libraries are keeping their users informed and keeping up on current developments and changes in the regulations. However, they do not have a significant change of policy related to recordkeeping and/or process. [71]

Another area of impact has been more of an administrative one for many cities and counties. Broward County, Florida, Board of County Commissioners on behalf of their citizens, passed a resolution "affirming the Bill of Rights and registering strong concerns about the Patriot Act. Broward is the 100th community to pass such a resolution

and the largest to have done so." Many cities and counties across the United States have passed similar resolutions to raise the awareness within Congress and to help influence legislation to limit some of the areas of concern within the Patriot Act. [99] Other cities and counties have passed even stronger language documents out-and-out opposing the Patriot Act. The City of Oakland's Police Department and Library Services sent an informational report, recommending acceptance of the City of Oakland's "Resolution to Oppose the Patriot Act and Related Executive Orders." The summary reflects the desire to have no citizen's civil rights or civil liberties infringed upon, and states that the steps included in the Patriot Act were "threatening civil liberties and basic freedom of residents…Oakland passed the resolution making it the 19th city in the nation to approve legislation directing City agencies to protect citizens from such practices as domestic spying, ethnic profiling, secret detentions, and the unauthorized release of personal records." [19]

At the state level, a specific issue involves the Nevada Motor Transport Association, probably similar to many other states, evaluating and implementing new processes related to background checks on drivers of hazardous materials in commerce and related Patriot Act implications. State agencies responsible for administration of the commercial driver's license are subject to new rules. Noncompliance by states can result in withholding of federal-aid highway funds. Coordination and definition is being provided by the Transportation Safety Administration (TSA). The TSA is also coordinating "with the Department of Justice (DOJ), The National Crime Prevention and Privacy Compact Council, states, and industry to develop an effective, efficient fingerprinting process. There is no specificity in the rules on this, other than the states

are responsible for administering the fingerprinting process." Also, the TSA will initiate background checks using currently available data sources (including information in CDLIS, NCIC-III, terrorism watch lists and others) on existing CDL license holders with hazmat (hazardous material) endorsements. All new license requests will follow the new expanded licensing/screening process. [72]

Federal Government/Agencies

There are significant impacts at the federal government level. These are as varied as the agencies in the federal government. Although many of these impacts overlap agencies and areas of concern, they have been grouped in general impact areas.

<u>Lists</u>

One summary level of information is related to the various lists and tracking information that are created, updated, and published in one form or another by the federal government. These lists, by and large, are used to review against an entity's source database to "flag" items for review and/or reporting. Some of the lists being maintained across the federal agencies and their basic uses include:

• The Terrorism Financial Review Group (TFRG) creates and updates a *Financial Control List*, which contains names and identifying data for individuals under investigation for potential links to terrorist organizations. These lists are regularly shared with domestic and international law enforcement and intelligence agencies, and with the Federal Reserve Board, which disseminates the lists to financial institutions so they can flag suspicious financial activity. [95]

•U.S. Treasury's *Specially Designated Nationals (SDN) List* often updated by Office of Foreign Asset Control (OFAC). [18]

•The Secretary of State has established *Money Laundering Watch List*, which identifies over 400 individuals worldwide who are known or suspected of money laundering. This list is checked by consular offices

and other federal officials before the issuance of visas for admission to the United States. [95]

•Under the Financial Action Task Force (FATF), in which Treasury and State participate, there is a process for designating countries that are noncooperating in the war against money laundering. This is the *List of Non-Cooperative Jurisdictions in the Global Fight Against Money Laundering*. [95]

•Under Section 1009, the FBI, the Transportation Security Administration (TSA), and the air carriers are coordinating to develop more sophisticated methods for transmission and use of the *List of Terrorists* suspected by the FBI and other U.S. government agencies. Electronic transmission of lists began immediately following 9/11. The FAA and currently the TSA issued and posted the lists on a secure Internet site accessible to regulated air carriers. In addition to comparison of passenger data against the suspected terrorist lists, the INS cross-checks international inbound passenger names against National Crime Information Center (NCIC) files. "Currently under study and/or development by the FBI, the TSA and the aviation industry, cooperatively with information management sectors, is the integration of existing technology and analytical software with passenger data, to compare it against risk assessors, including terrorist lists, and other databases to identify potential matches." [85]

Information Sharing

Another summary area of implementation focuses on sharing of information across agencies. Prior to the Patriot Act, there was information exchange and sharing, however, it was usually specific to certain cases, or certain investigations. Since the Patriot Act, based on the legislation, agencies can cooperatively coordinate data and information to identify patterns and see "the whole picture" versus trying to piece it all together separately.

One expansive area of implementation affects visas and creating a coordinated effort between the FBI, the INS, and the State Department. A specific area of information sharing relative to visas involves an Interagency Working Group (IWG) formed by representatives of the Department of Justice (DOJ) and the Department of State (DOS). The group is working to coordinate implementation of the Visa Waiver Program (VWP), including an aspect about requiring machine-readable passports. "In addition, the INS' Forensic Document Laboratory continues to work closely with the DOS Bureau of Consular Affair's Fraud Prevention Program to disseminate fraud reports and antifraud recommendations, which many VWP countries have found helpful in protecting the integrity of their passports." [85]

Another area of information sharing is based on a directive by the Attorney General on coordination of information relating to terrorism. This directive focused on the investigative components of the DOJ establishing procedures to systematically and regularly provide names, photographs (if available) and other related data for known or suspected terrorists to be included in the following databases:

Department of State TIPOFF System – designed to detect known or suspected terrorists who are not U.S. Citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points.
FBI National Crime Information Center (NCIC). The NCIC is the nations principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 U.S. local, state and federal law enforcement officers.

• The U.S. Customs Service Interagency Border Inspection System (IBIS). This system is the primary automated screening tool used by both the INS and U.S. Customs Service at ports-of-entry." [85]

Another related but separate example of information sharing relates to the "incorporation of the Advance Passenger Information System (APIS), a subsystem of the IBIS system to provide NCIC III data on alien passengers to INS officers at air ports-ofentry." This would allow an advance screening against the data and may flag at an earlier point those passengers showing up on the various databases, thus allowing the INS officers to be alerted of potential issues. [85] An additional specific file/information sharing example includes the "FBI's Criminal Justice Information Systems Division (CJIS) has provided databases to the DOS for inclusion in their CLASS database. Also, CJIS has provided an Integrated Automated Fingerprint Identification System (IAFIS) extract of 83,000 fingerprint based records of Wanted Persons having foreign places of birth for inclusion in the Automated Biometric Identification System (IDENT). CJIS has also provided INS with two CDs containing information regarding military detainees in Afghanistan and Pakistan, as well as those detained at Guantanamo Bay, Cuba. In addition per a memorandum of understanding between the DOS and FBI-CJIS, extracts are provided from the NCIC's Deported Felon File, Foreign Fugitive File, and the Violent Gang and Terrorist Organizations File. Monthly updates from these files are ongoing. As of report date 8/26/02, NCIC records to date are approximately 425,000 and the III records are almost 8 million." [85]

Information sharing can also be international. The U.S. Secretary of State is sharing visa lookout information related to crime and terrorism records in the State Department's databases with foreign governments. The State Department is pursuing agreements with foreign governments to put more of these information exchanges in place. Until the actual agreements are signed, preliminary steps are being taken to build a framework to proceed. While the formalities continue, a working draft of a process "identifies types of information to be shared, addresses the extent to which information may be shared with other agencies, and provides a mechanism for systems interface modifications as technical upgrades warrant. Once an agreement is reached, it will be a template for database sharing accords with other governments." [85]

Integrated Entry and Exit

Another overall project relates to an integrated entry and exit data system for airports, seaports, and land-border ports of entry. Section 414 relates to implementing a task force to coordinate this process and to define the additional processes necessary to meet the requirements of the Patriot Act. The "INS has established a multi-agency Program Management Office to coordinate all activity associated with this effort, including infrastructure enhancements." [85] External departments involved in this project include Office of Homeland Security, Office of Science and Technology Policy, National Institute of Standards and Technology, and Data Management Improvement Act (DMIA) Task Force. Internally, the INS has formed the Entry Exit Program Team (EEPT) to implement a border management program that includes an automated information system. To give an example of how expansive a program like this is, below is the list of the organizations included on this team:

INS – Office of Inspections
INS – Office of Strategic Information and Technology Development
INS – Office of Information Resources Management
INS – Office of General Counsel
INS – Office of Facilities
INS – Office of Immigration Services
INS – Office of Public Affairs and Congressional Relations
Dept. of State – Bureau of Consular Affairs
Dept. of Transportation – Transportation Security Administration
Dept. of Justice – Justice Management Division
U.S. Customs Service – Field Operations

The "implementation of the Entry Exit System will follow an evolutionary,

incremental model wherein planned 'phases' will be used to scale, insert technology and generally enhance the system's functionality. The following deadlines are legislatively mandated:

10/1/02 – Entry Exit System operational at all air and sea POEs for visa waiver program travelers
12/31/03 – Entry Exit System operational for all travelers at all air and sea POEs
12/31/04 – Entry Exit System at the 50 largest land POEs
12/31/05 – Entry Exit System operational at all POEs for all travelers"

In conjunction with the Integrated Entry and Exit projects is an increased focus on the use of biometric technology and the development of tamper-resistant documents readable at ports of entry. Information and direction related to a study of biometric identifiers is elaborated further in section 1008.

Border Control

Related to an Integrated Entry and Exit process, but very particular to implementation processes at the borders are some specific projects. Authorization was granted to increase the number of inspectors for the Northern Border (some of the Northern Border sites impacted include Spokane, WA; Grand Forks, ND; Detroit, MI; and Buffalo, NY among others). An additional 245 positions were authorized, and hiring was to be completed as of March 2003. Beyond adding resources, training capacity has been emphasized. The Immigration Officer Academy (IOA) has expanded the number of classes it is offering by expanding its schedule to train six days a week. It is also expanding the locations of training in order to facilitate further increases in classes.

Another area of focus was on improving technology for monitoring the Northern Border. Some related projects included installing the Integrated Intelligence Surveillance System (ISIS) at 55 Northern Border sites; deploying new equipment like helicopters to increase air surveillance hours to the Northern Border areas; availing Border Patrol

Agents to 500 additional Infrared Scopes for improved night vision capabilities; and implementing redundant and backup system processes for the IDENT system in order to assure system availability even under emergency situations. [85]

Another area of improvement for border control related to improving and integrating systems. Following the passage of the Patriot Act, the need for utilizing rapid-capture flat fingerprint devises for visa and passport purposes put an increased emphasis on a study that was already underway. A final report on the study was comprised from five component tests: Ohio Web Check Pilot Project, Texas Flat-print Initiative, FBI Internal Flat Verses Rolled Testing, Latent Testing, National Institute of Standards and Technology (NIST) Testing. The information from the study, in conjunction with an Algorithm Test Bed (ATB) purchased from Lockheed Martin Information Systems for additional testing of the IAFIS will certify the information and vastly improve the accuracy of the IAFIS system. [85]

For the past several years, a planned project to integrate the INS' IDENT system with the FBI's IAFIS system has been ongoing. The IDENT/IAFIS Integration Project is designed to give the INS the ability to determine whether a person they have arrested is wanted by law enforcement, was previously deported, or has a criminal record in the FBI's master file. Recent funding will allow for deployment in 30 locations (including northern border sites); "systems engineering (to permit simultaneous search of both systems and system upgrades; research and development of alternative fingerprinting systems; the development and analysis of performance measures; and program management and planning." [85] Currently, an interim IDENT/IAFIS solution is being implemented requiring individuals to be processed two times: once under the IDENT
system, and once using a sped up IAFIS check. Beyond this, the Department is in process of creating a way for INS to take 10 rolled fingerprints and concurrently search both systems. Full integration of the IDENT and IAFIS systems is underway, however it could take up to five years. As a further interim solution, the INS recently added approximately 100,000 records to IDENT for persons probable to be encountered by INS who are wanted by federal, state, and local law enforcement. Just this step, has immensely improved the INS's capability to intercept criminal fugitives. Since January 1, 2002, (report in July 2002) these efforts have led to the identification of around 1,800 individuals who were wanted for various offenses including homicide, rape, drug crimes, and parole violations. [85]

Financial Monitoring

One area that already had significant controls, which has expanded substantially with the Patriot Act is monitoring financial activities and coordinating between the financial institutions and the federal agencies.

There is a new interagency, Terrorism Financial Review Group (TFRG), operating out of FBI Headquarters. The TFRG is bringing together extensive databases and the expertise of numerous federal agencies to focus on the financial aspects of the terrorists' organizations.

"The TFRG was formed with a two-fold mission. First, it was designed to conduct a comprehensive financial analysis of the 19 hijackers to link them together and to identify their financial support structure within the United States and abroad. Second, it was designed as a template for preventative and predictive terrorist financial investigations. And the mission of the TFRG has since evolved into a broader effort to identify, to investigate, to prosecute, to disrupt, and to dismantle terrorist-related financial and fund-raising activities. For instance, it conducts full financial analyses of terrorist suspects and their global financial support structures; coordinates liaison and outreach efforts to exploit financial resources of private, government, and foreign entities along with the Treasury

Dept.: uses FBI and LEGAT expertise and relationships to develop financial information from foreign law enforcement and private agencies; works jointly with the law enforcement, regulatory and intelligence communities; develops predictive models and mines data to proactively identify terrorist suspects. The TFRG has conducted outreach programs to share information with the financial community and with law enforcement. It has developed numerous data mining projects to provide further predictive abilities and to maximize the use of both public and private database information. These efforts are complemented by the centralized terrorist financial database which the TFRG has developed. This information is used to identify terrorist cells operating in the United States and abroad to prevent further terrorist acts. The TFRG created and updates a financial control list, which contains names and identifying data for individuals under investigation for potential links to terrorist organizations. These lists are regularly shared with domestic and international law enforcement and intelligence agencies, and with the Federal Reserve Board, which disseminates the lists to financial institutions so they can flag suspicious financial activity. Further, the TFRG is working with FinCEN to explore new ways to data mine the suspicious activity report, and the currency transaction report, and the currency and monetary instrument report databases." [95]

A specific area of financial control relates to FinCEN (Financial Central) establishing a secure network and the Patriot Act Communication System (PACS) to enable online filing of SARs and CTRs and to provide financial institutions with alerts and reports of suspicious activities. SARs filings are Suspicious Activity Reports to FinCEN that help to enhance the liaison relationship between law enforcement and financial services. CTR filings are currency transaction reports to FinCEN. [95]

Pertaining to certain types of accounts, new requirements abound for more thorough due diligence and review of correspondent accounts and private banking accounts. Financial institutions must implement and monitor thorough procedures that will be able to detect and report money laundering on foreign customers and international accounts. Also required is ongoing review of the FATF's list of non-cooperative jurisdictions in the global fight against money laundering. [80] The Federal Reserve Bank Board has submitted letters of instruction to Officer in Charge of Supervision at each Federal Reserve Bank. In these letters, new process and procedures related to section 327 of the Patriot Act, dealing with validating banks, acquiring banks, and new banking relationships, will be reviewed thoroughly on both sides of transactions for compliance with anti-money laundering laws and regulations. This includes more intense scrutiny when foreign banks are involved in a transaction. [39]

Control Processes

As the Patriot Act was implemented, specific controls evolved to allow for and require monitoring, evaluation, and reporting of issues related to the Patriot Act. A few of the specific examples found in research relate to two departments/areas within the Department of Justice: the Office of the Inspector General and the Office of Attorney General.

The Office of Inspector General is responsible for reviewing programs and personnel in all DOJ components including FBI, DEA, Bureau of Prisons (BOP), Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), U.S. Attorney's Office, and other DOJ Components. Section 1001 of the Patriot Act elaborates on reviews of claims related to civil rights or civil liberties violations by DOJ employees. Additional reviews of specific areas of concern and related process and policies within any area under the review list can be initiated by the OIG. In addition, the OIG must publicize and communicate via their semi-annual report, and through advertising on television, radio, Internet, and flyers. These publications and communications are intended to raise awareness of the process and steps for contacting the agency on issues. [85]

The Office of the Attorney General requires reports to Congress. These reports are answers to questions regarding the implementation of the Patriot Act, as posed by

75

various members of Congress and special committees. The answers elaborate on status information, progress to-date, and various related information.

Universities and Schools

Foreign student monitoring and no-show reporting by schools are two areas now expanded by the Patriot Act. Section 416 directs the Attorney General to implement fully the foreign student-monitoring program, and to expand that program to include other approved educational institutions like flight, language training, or vocational schools. [85, 6]

"The foreign student monitoring program system is the Student and Exchange Visitor Information System (SEVIS). SEVIS is an Internet-based system that provides tracking and monitoring functionality, with access to accurate and current information on non-immigrant students (F and M visa) and exchange visitors (J visa), and their dependents (F2, M2 and J-2). SEVIS enables schools and program sponsors to transmit electronic information and event notifications, via the Internet to the Immigration and Naturalization Services (INS) and Department of State (DOS) throughout a student's or exchange visitor's stay in the United States." [85]

Some steps taken to implement SEVIS include development and distribution of

SEVIS training materials and completion of INS field officer training sessions. Related are the development of a designated school official (DSO) requirement outline of roles and responsibilities and coordination with the schools. Another step is initiation of a competitive process to select contractors to assist with the certification of schools prior to enrollment in SEVIS.

"Investigations resulting from information received regarding those students who do not arrive at the intended school are conducted at the local level by the INS district office having geographic jurisdiction. However, INS has established a centralized electronic mailbox (Investigations – SEVIS Reports) to receive reports from educational institutions participating in SEVIS of out of status students including those who fail to appear. The information received in the electronic mailbox is reviewed to determine which INS district office would receive the information provided for follow-up inquiry. INS is currently in the process of developing and reviewing internal proposals to establish a method to review and analyze the incoming material in conjunction with other law enforcement databases and other information sources prior to dissemination for possible enforcement action. Immigration law enforcement actions can then be prioritized in accordance with public safety interests, immigration system integrity, and resource considerations. It is anticipated that when fully operational, SEVIS will generate 50,000 to 60,000 referrals of out of status students, including those who fail to appear. This raises concerns regarding INS Investigative resources to accomplish this task along with existing functions." [85]

As an example, Boson University currently has a paper process for their oncampus and federal filings to track their F-1 and J-1 students, and their J-1 scholars. All of the data for these activities resides in over 50 offices throughout their campuses. There is no centralized source of data and no electronic data links between the offices needing them. In the past two decades only incidental reporting has been required based on the filing of forms. All future processing must be done via SEVIS, the INS' application available on the Internet, and the process will migrate away from the papercentric processes to electronic data transfer. Also, reporting will now be continuous, event-based requiring much more information gathered per student. Also, there will likely be a federal recertification process for schools and exchange visitor programs implemented in the near future. On a related note, "it is probably only a matter of time before an INS-issued secure ID card, containing biometric identifiers, will be required of all students and exchange visitors. This ID card will likely facilitate visa issuance and/or reissuance, U.S. entry and/or reentry, and INS benefit processing." [6]

The impacts to government at all levels are extensive. The task underway and ahead of all areas of the government is daunting, especially in the face of the additional pressures of tough economic times. Trying to improve and enhance processes is difficult,

77

but trying to do it with limited resources is that much worse. At the federal level, and across all levels in some instances, funding has been provided to enable the development and implementation of the required processes. Regardless, an area of improvement already witnessed is the improved open communication and information sharing amongst agencies and organizations within all levels of government.

VI. Conclusions

The Patriot Act is a far-reaching piece of legislation that amends a variety of previous laws and regulations. Impacts of the Patriot Act are as wide sweeping as the Act itself. This paper has worked to identify the impacts, positive and negative, to businesses and government entities and particularly focus on the Information Technology and Computer Information Systems impacts of the Patriot Act. The range of technology impacts varies from as simple as list distribution and review to complex algorithm programs to new scenario evaluation programs to complex data mining processes. Entire departments and agencies within government have been merged, and interagency communication is becoming the norm. Similar impacts to businesses – communication between businesses and with the government and regulatory agencies - are evolving as the ongoing implementations of this Patriot Act proceed and evolve. Based on our review, the impacts of the Patriot Act will be seen and felt for many years to come.

78

VII. Works Cited

- 1. Abramson, Larry, "Frazzled Travelers Fight to Clear Their Names," <u>http://discover.npr.org/features/feature.jhtml?wfld=1233255</u> All Things Considered audio April 15, 2003.
- 2. ACLU. How the USA-PATRIOT Act Limits Judicail Oversight of Telephone and Internet Surveillance. <u>http://archive.aclu.org/congress/l102301g.html</u>
- 3. Baeza Bickel, Nardy. ACLU forum questions Patriot Act. The Grand Rapids Press. September 4, 2003. Page A21.
- 4. Bankers Systems and VMP Mortgage Solutions Strengthen Fraud Management Technology for Mortgage Lenders. Computer/Electronic News. <u>http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=SVBIZINK3.story&STORY=/www/story/09-17-2003/0002018789&EDATE=WED+Sep+17+2003,+08:03+AM</u>
- 5. Blakeman, Ramie. Section 326: a course of action. Part 1 An Overview of CIP. Legal & Compliance Director. © Bridger Systems, Inc. 2003.
- 6. Boston University International Students & Scholars Office <u>www.bu.edu/isso/sevis/background/patriot-act/</u>
- 7. Bridger Systems. <u>http://ofaccompliance.com/</u> <u>http://ofaccompliance.com/education-community-banker-options.htm</u>
- 8. Broadwell, Hunter and Parker, Ashley. *Patriot Act: Online Implications*. http://www.unc.edu/courses/2003spring/law/357c/001/projects/hunterb/Patriotact/
- 9. Burriesci, Jeanette. "The Price of Protection". <u>Intelligent Enterprise</u>. San Mateo: Aug 10, 2003. Vol. 6, Iss. 13; pg. 8.
- 10. Bureau of National Affairs, "Lockheed Gets TSA CAPPS II Contract" <u>http://subscript.bna.com/SAMPLES/fcr.nsf/18f5159fe53d0fb185256743006e4387</u> <u>/de702fcce9d596b185256ce60006e882?OpenDocument</u> Volume 79 Number 10 Tuesday, March 11, 2003 ISSN 1523-5696 Page 300.
- 11. Burns, Margie, "Another Fortunate Bush Brother" http://www.counterpunch.org/burns1205.html December 5th, 2002.
- <u>12.</u> Butler, John. *Striving to Increase Satisfaction*. <u>http://www.rbg.com/images/autosp03.pdf</u>
- 13. CDT (Center for Democracy and Technology). The New Homeland Security Department Challenge, Potential and Risk Privacy Guidelines, Careful

Oversight Required. Dec. 10, 2002. http://www.cdt.org/security/homelandsecuritydept/021210cdt.shtml

- 14. Celent, "Ranking the vendors of Anti-Money Laundering," July 11, 2003. http://www.celent.com/pressreleases/20030711/AMLVendors.htm
- 15. Center for Democracy and Technology: http://www.cdt.org/security/010911response.shtml
- 16. Chabrow, Eric, "Patriot Act Spurs New Software for Colleges," Autust 26, 2002, http://www.informationweek.com/story/showArticle.jhtml?aritlceEd=6502956
- 17. Chiara, Margaret M. United States Attorney Western District of Michigan. Patriot Act is no threat to liberties. Grand Rapids Press. Sept. 14, 2003.
- 18. Chudnow, Christine Taylor. Computer Technology Review U.S. Gets Tough on Terror with Patriot Act
- 19. City of Oakland <u>www.oaklandnet.com/government/council/reports/06-17-</u>03/council/26rpt.pdf
- Cividanes, Milo. Halpert, Jim. Plesser, Ron. Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001. E-Commerce & Privacy Group. October 31, 2001. <u>http://www.cdt.org/security/011031summary.shtml</u>
- Colkin Cuneo, Eileen. Beyond Compliance. <u>Wall Street & Technology</u>. New York: May 2003. pg. 20, 3 pgs
- 22. Cornehls, Jim. The USA Patriot Act: The Assault on Civil Liberties. Zmag. July 31, 2003. <u>http://www.globalpolicy.org/wtc/liberties/2003/0806patriot.htm</u>
- 23. Costlow, Terry. U.S. Security and Public Privacy: Where Do the Lines Get Drawn? Today's Engineer <u>http://www.todaysengineer.org/archives/pp_archives/mar02/pp1.htm</u>
- 24. CRS Report for Congress RL31289. The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government (PDF), updated March 4, 2002. <u>http://www.epic.org/privacy/terrorism/usapatriot/RL31289.pdf</u>
- 25. Cuneo, Eileen Colkin. "Beyond compliance," <u>Wall Street & Technology</u>. New York: May 2003 PG 20, 3 pgs.
- 26. Daily Rotten. *Patriot Act II (draft)*. <u>http://www.dailyrotten.com/source-docs/patriot2draft.html</u>
- 27. Davis, Sharon L. Profiling Terror. Draft. http://www.isrcl.org/Papers/Davies.pdf
- Electronic Frontier Foundation Analysis Of The Provisions Of The USA Patriot Act That Relate To Online Activities (Oct 31, 2001)

http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_p atriot_analysis.php

- 29. Electronic Privacy Information Center. The USA Patriot Act. September 15, 2003. <u>http://www.epic.org/privacy/terrorism/usapatriot/</u>
- 30. Electronic Privacy Information Center. FBI's Carnivore System Disrupted Anti-Terror Investigation. <u>http://www.epic.org/privacy/carnivore/5_02_release.html</u>
- 31. Electronic Privacy Information Center. Privacy and Consumer Profiling. http://www.epic.org/privacy/profiling/
- 32. Experian, "Best Practices for preventing fraud losses and protecting customers from identity theft," White Paper. <u>www.experian.com</u>
- 33. Fausett, Bret A. Becoming a Patriot, http://www.newarchitect.com/archives/2002/02/legal/
- 34. Feingold, Russ, "Civil Rights: Post-September 11th World," August 4, 2003 <u>Http://feingold.senate.gov/issues_civil_post_sept11.html</u>
- <u>35.</u> FinCEN. Assessment of Civil Money Penalty with Undertakings. http://www.fincen.gov/western_union_assessment.pdf
- 36. Fincentric Corporation: Fincentric and Interlink Electronics join forces at Rainier Pacific Bank to provide increased automation and security (C) M2 COMMUNICATIONS LTD, M2 PRESSWIRE, 20 August 2003.
- 37. Fornaris, Carl A.; Gomez, Ileana; Horn, Alan B. *GT Alert: USA Patriot Act Final Regulations that apply to Casinos and Card Clubs.* <u>http://www.gtlaw.com/pub/alerts/2002/horna_09a.asp</u>
- 38. Fornaris, Carl A.; Gomez, Ileana; Horn, Alan B. GT Alert: USA Patriot Act -Proposed Regulations Affecting Insurance Companies. <u>http://www.gtlaw.com/pub/alerts/2002/horna_09c.asp</u>
- 39. FRB Supervisory Letter SR.02-8 on Implementation of Section 327 of the USA PATRIOT Act – www.federalreserve.gov/boarddocs/SRLETTERS/2002/sr0208.htm
- 40. Glaberson, William. Racial Profiling May Get Wider Approval by Courts. New York Time. September 21, 2001. <u>http://www.crimelynx.com/racpro.html</u>
- 41. Gustafson (1), Samuel H. Interview of an Insurance Company Programmer.
- 42. Gustafson (2), Samuel H. Interview of Donalyn Sandborn, IT Administrator of a Credit Union.

- 43. GVSU Patriot Act Forum, GVSU Loosemore Auditorium, September 18, 2003
- 44. Harden, Blaine, "Two on 'No-Fly' List Arrested at Airport," August 14, 2003, p. A02, <u>http://www.washingtonpost.com/ac2/wp-dyn/A55758-2003Aug13?language=printer</u>
- 45. Harrison, Ann. Behind the USA Patriot Act By, <u>AlterNet</u>. November 5, 2001. <u>http://www.alternet.org/story.html?StoryID=11854</u>
- 46. Hoffman, Thomas, "IT departments face alack of project management knowhow," August 11, 2003, Vol. 37, Iss. 32, pg 16. King, Nancy J. Electronic Monitoring: How far can you go? A briefing for corporate managers 1. <u>http://www.forensics-intl.com/art19.html</u>
- 47. IBM Websphere Business Intigration for Banking http://www-3.ibm.com/software/integration/wbisolutions/banking/usapatriot.html
- 48. Informatica. *Getting Ready for Sarbanes-Oxley and Patriot Act Audits:* Leveraging Integrations for Better Visibility. <u>http://www.informatica.com/Solutions/sarbanes+oxley/sp_informaticafinala.pdf</u>
- 49. InfoSec Links http://www.issa-dv.org/resources/web/links/
- 50. Innovative Systems Launches Online USA PATRIOT Act Compliance Solution <u>http://www.prnewswire.com/cgi-</u> <u>bin/stories.pl?ACCT=SVBIZINK3.story&STORY=/www/story/09-18-</u> 2003/0002019847&EDATE=THU+Sep+18+2003,+10:00+AM
- 51. Intemann, Leslie. Patriot Act has implications for information technology at universities. Dec. 6, 2001.<u>http://www.cit.cornell.edu/computer/news/featurestoc/patriot.html</u>
- 52. Kellner, Tomas, "Banks Taken To Cleaners In Terrorist Search," http://www.forbes.com/2003/05/14/cz_tk_0512money.html - 69k - Sep 26, 2003
- 53. Kellner, Tomas, "The Best Anti-Money-Laundering Technology," 8.1.03, http://www.forbes.com/2003/08/01/cz_tk_07xxantimoney.html
- 54. Kerr, Dr. Donald M. Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director. Center for Democracy and Technology <u>http://www.cdt.org/security/carnivore/</u>
- 55. King, Nancy J. Electronic Monitoring to Promote National Security Impacts Workplace Privacy. *Employee Responsibilities and Rights Journal*, Vol. 15, No.
 3, September 2003. <u>http://www.cob.sjsu.edu/malos_s/Privacy%20and%20National%20Security.pdf</u>

- 56. Krebs, Brian. Mail Tracking System Raises Privacy Fears. August 7, 2003. <u>http://www.washingtonpost.com/ac2/wp-</u> <u>dyn?pagename=article&node=&contentId=A29130-2003Aug7¬Found=true</u>
- 57. Kuchinskas, Susan. *PayPal's Hands Are Clean, Business Still Booming*. <u>http://siliconvalley.internet.com/news/article.php/2240641</u>
- 58. Leahy, Senator Patrick. Section-by-Section summary of USA-PATRIOT Act
- 59. Lilenthal, Steve, "Complexities Of Federal Data Mining". July 15, 2003. www.freecongress.org/commentaries/030715SL.asp
- 60. Lindorff, Dave. Grounded. Salon Magazine. Nov. 15, 2002. http://www.salon.com/news/feature/2002/11/15/no_fly/print.html
- 61. Lydersen, Kari, "USA: Spying for Fun and Profit," May 28th, 2003. http://www.corpwatch.org/news/PND.jsp?articleid=6869
- 62. Maiello, Michael, "Citigroup's Low-Tech USA Patriot Act Solution," http://www.forbes.com/execpicks/2003/09/08/cz. mm_0908citi.html, 09.08.03.
- 63. Mantas. http://www.mantas.com/products
- 64. Mantas Inc. "Understanding Behavior Detection Technology: Emerging Approaches To Dealing With Three Major Consumer Protection Threats," A White Paper by Mantas. <u>www.mantas.com</u> April 2003.
- 65. Markle Task Force on National Security in the Information Age: <u>http://www.markletaskforce.org</u>
- 66. Mearian, Lucas, "Brokerages face big IT bill to comply with USA Patriot Act, March 17, 2003. elab.vanderbilt.edu/.../pdf/student_projects/ Calculating%20the%20Cost%20of%20Privacy%20-%20Final%20Report.pdf
- 67. Mitchell, Louise, "The Implications of the USA Patriot Act on Foreign Banking Institutions," <u>www.stvincentoffshore.com/pdf/USA%20Patiot%20Act.pdf</u> May 24, 2002.
- 68. Mitchell, Kevin. Engineering Manager for Iserv. Interview: 10/22/03.
- <u>69.</u> MJSA Manufacturing Jewelers and Suppliers of America. *MJSA Issue Papers:* USA Patriot Act. <u>http://mjsa.polygon.net/gov/issue_papers/patriot_act.php</u>
- 70. Moyers, Scott. Patriot Act asks banks to collect more personal information http://www.semissourian.com/story.html\$rec=119928

- 71. Multnomah County Library USA PATRIOT Act & Library Confidentiality Q & A <u>www.multcolib.org/news/patriotact.html</u>
- 72. Nevada Motor Transport Association www.nmta.com/Hazmat%20Security%20Plan/Analysis%20Summary.html
- 73. OSU to Explore Impact of Terrorism with "War on Main Street" http://oregonstate.edu/dept/ncs/newsarch/2003/Mar03/mainstreet.htm
- 74. Palast, Gregory. Florida's flawed "voter-cleansing" program. http://dir.salon.com/politics/feature/2000/12/04/voter_file/index.html
- Pallay, Jessica. "Partners against Crime." Information Week. Manhasset: Aug 4-Aug 11,2003. Iss. 950; pg. 80
- 76. Pallay, Jessica. "The New Dream Team." <u>Wall Street & Technology</u>. New York: Jul 2003. Vol. 21, Iss. 7; pg. 51
- 77. The Patriot Act. <u>http://www.epic.org/privacy/terrorism/hr3162.html</u> & <u>http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf</u>
- 78. Patriot Act means major technology investment. *Anonymous*. <u>Wall Street & Technology</u>. New York: Jun 2003. pg. 12.
- 79. Pierre, Robert E. Botched Name Purge Denied Some the Right to Vote. Washington Post. Thursday, May 31, 2001; Page A01. <u>http://www.washingtonpost.com/ac2/wp-dyn/A99749-2001May30</u>
- 80. PO-1082 Under Secretary Gurule' Remarks on PATRIOT ACT <u>www.ustreas.gov/press/releases/po1082.htm</u>
- 81. Ramasastry, Anita. Patriot II: The Sequel Why It's Even Scarier than the First Patriot Act. <u>http://writ.news.findlaw.com/ramasastry/20030217.html</u>
- 82. Reese, Charley. Nothing patriotic about the Patriot Act. The Grand Rapids Press. August 29, 2003. Page A11.
- 83. Regis Hyle, Robert. Clean Sweep. Tech Decisions for Insurance Companies. Sept. 2002. http://www.technologydecisions.com/backissue/0902/9 18 02 11.asp
- 84. Regulatory Governance and Beyond: How Data Mirror Solutions Support Compliance Efforts <u>http://www.datamirror.com/resourcecenter/newsletter/</u>
- 85. Report on Implementation of the USA PATRIOT Act: Justice Department to Congress <u>www.fas.org/irp/news/2002/10/doj101702.html</u>

- 86. Ridder, Knight. Memo shows US has not used Patriot Act to seek library data By, 9/18/2003.<u>http://www.boston.com/news/nation/washington/articles/2003/09/18/m</u> emo shows us has not used patriot act to seek library data/
- 87. River City Credit Union. Are There Penalties for Non-Compliance? http://www.rivercu.com/adobe/PatriotActINSIDE.pdf
- 88. Rose, Laurie. Moorman, Mark. "The USA PATRIOT Act: A Long-Term Financial Services Strategy," May 16th, 2003. <u>http://www.technologyforfinance.com/FeatureRO.asp?FeatureId=72</u>
- 89. Royle, Bill. Patriot Act II: An interview with EFF's Cindy Cohn. April 24, 2003. http://www.techfocus.org/comments.php?id=3101&catid=34
- 90. Russell, David Williams. *A Banker's Overview of the USA Patriot Act.* http://www.boselaw.com/articles/Russell HoosBank 03.pdf
- 91. Salkever, Alex. We've Made Bad Security Tradeoffs. Author Bruce Schneier discusses why the Patriot Act and other anti-terror measures mean "giving up a lot -- and not getting very much" http://www.businessweek.com/technology/content/sep2003/tc2003092_0578.htm
- 92. Sheshunoff Newsletter. *BSA Compliance Trips Up Western Union*. <u>http://www.sheshunoff.com/email/archive/0403/oper_new3.html</u>
- 93. State of New York Banking Department. Press Release Banking Department Fines Western Union \$8 Million for Violating Bank Secrecy, USA Patriot, New York Banking Laws. http://www.banking.state.ny.us/pr021218.htm
- 94. Sybase Software for complying with Patriot Act. Has other good links. http://www.sybase.com/solutions/patriotact
- 95. Terrorist Financing Implementation of USA PATRIOT Act http://commdocs.house.gov/committees/bank/hba83586.000/hba83586_0.htm
- 96. Tompkins, Joseph B., "The Impact of the USA Patriot Act of 2001 on Non-U.S. Banks," <u>www.imf.org/external/np/leg/sem/2002/cdmfl/eng/tompki.pdf</u> Washington, DC, May 7, 2002.
- 97. Towns, Douglas. Legal Issues Involved in Monitoring Employees' Internet and E-Mail Usage. GigaLaw.com January 2002. <u>http://www.gigalaw.com/articles/2002-all/towns-2002-01-all.html</u>.
- 98. TradePoint's Regulatory Compliance System http://www.tradepointsystems.com/USA/product.htm

- 99. Truthout Special: Patriot Act Resolution Passed in Broward Florida <u>http://truthout.org/docs_03/051003E</u>
- 100. "TSA's CAPPS II Gives Equal Weight to Privacy Security," March 11, 2003, <u>http://www.tsa.gov/pubic/display?content=250</u>
- 101. TSA, Transportation Security Administration, Department of Homeland Security "Privacy Act of 1974: System of Records," Washington, D.C., July 22, 2003 www.epic.org/privacy/airtravel/capps-notice.pdf
- 102. The USA PATRIOT Act: Preserving Life and Liberty. http://www.lifeandliberty.gov/
- 103. USDOJ OIG. Report to Congress on Implementation of Section 1001 of USA PATRIOT Act – <u>www.usdoj.gov/oig/special/03-07/final.pdf</u>
- 104. Ward, Elaine N. USA PATRIOT Act of 2001. ITS Information Security Office. Feb. 7, 2002. <u>http://www.utexas.edu/computer/news/features/0202/patriotact.html</u>
- 105. Wilson, Lizette, "Software firms get boost from Patriot Act," July 22, 2002, East Bay Business Times, http://eastbay.bixfournals.com/eastbay/stories/2002/07/22/sotry7.html
- 106. Vollmer, Jennifer. Ingram, Lauri. Training, E-Learning, and Compliance. October 28, 2002. <u>http://www.metagroup.com/cgi-bin/inetcgi/jsp/displayArticle.do?oid=33753</u>
- 107. United States General Accounting Office. Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing. Information Technology. April 2003. <u>http://www.gao.gov/highlights/d03322high.pdf</u>

Appendix A

A Description and Overview of selected sections of the USA PATRIOT Act.

The following are brief overviews of the sections of the Patriot Act that have an impact on computing. These overviews were originally presented in *Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001* by the E-Commerce & Privacy Group written by Ron Plesser, Jim Halpert, & Milo Civivanes on October 31, 2001. We have since updated these overviews to include all new details that have surfaced over the last two years since the original overviews written by the authors cited above. Brief summery of selected sections with detailed summery to follow:

- Section 103 Increased Funding to FBI's Support Center.
- Section 202 Authority to intercept wire, oral, or electronic communications relating to computer fraud and abuse offenses.
- Section 203 Authority to share criminal investigation information.
- Section 204 Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.
- Section 206 Roving Surveillance authority under the Foreign Intelligence Surveillance Act of 1978.
- Section 209 Seizure of voice mail messages pursuant to warrants.
- Section 210 Scope of subpoenas for records of electronic communications.
- Section 211 Clarification of scope.
- Section 212 Emergency disclosure of electronic communications to protect life and limb.
- Section 214 Pen register and trap-and-trace authority under FISA.
- Section 215 Access to records and other items under the Foreign Intelligence Surveillance Act.
- Section 216 Modification of authorities relating to the use of pen registers and trap-and-trace devices.
- Section 217 Interpretation of computer trespasser communications.
- Section 218 Foreign intelligence information requirement for FISA authority.
- Section 219 Single-jurisdiction search warrants for terrorism.

- Section 220 Nationwide service of search warrants for electronic evidence.
- Section 222 Assistance to Law enforcement agencies.
- Section 223 Civil liability for certain unauthorized disclosures.
- Section 224 Sunset.
- Section 225 Immunity for compliance with FISA wiretap.
- Section 326 Verification of identification.
- Section 351-361 Bank Secrecy Act amendments and related improvements.
- Section 414 Visa integrity and security.
- Section 503 Collection of DNA identification of terrorists and other violent offenders.
- Section 507 Disclosure of educational records.
- Section 701 Expansion of regional information sharing system.
- Section 808 Provides the definitions for the Federal crime of terrorism.
- Section 814 Deterrence and prevention of cyber-terrorism.
- Section 815 Additional defense to civil actions relating to preserving records in response to government requests.
- Section 816 Development and support of cyber security forensic capabilities.
- Section 1001 USDOJ OIG handling of claims of civil rights or civil liberties violations allegedly committed by DOJ employees.
- Section 1009 Feasibility of providing airlines with computer access to the names of suspected terrorists.
- Section 1016 Critical infrastructures protection.

Section 103

This provides for increased funding for the FBI's technical support center. Significantly more money will be spent on electronic surveillance by the government. This section authorizes \$200 million each year for the fiscal years 2002, 2003, and 2004 for the FBI's technical support center. The center is a principal source of government technical surveillance initiatives, and this funding could accelerate more such proposals.

Section 202

This expands the authority to intercept wire, oral, or electronic communications relating to computer fraud and abuse offenses. Additionally, this expands the ability for service providers to get government help with hacking, denial of service attacks, and related Computer Fraud and Abuse Act violations. It also adds the Computer Fraud and Abuse Act offenses to the list of predicates for obtaining Title III wiretaps, thereby facilitating government investigation of hacking offenses.

Section 203

This provides additional authority to share criminal investigative information with different government agencies. Information obtained from grand juries and wiretaps will be accessible to a wider range of government offices and officials. This section amends the Federal Rules of Criminal Procedure and 18 U.S.C. § 2517 to allow intelligence information obtained in grand jury proceedings and from wiretaps to be shared with any federal law enforcement, protective, intelligence, immigration, and national defense or security personnel, provided that recipients of information could only use such information in connection with their official duties and subject to the disclosure limitations in existing law. In the case of grand jury information, it would require notification to the court after disclosure.

Although this section broadens the categories of individuals with whom criminal investigative information can be shared, it was narrowed in the legislative process to require these individuals to use this information only in connection with their official duties.

Section 204

This is the clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications. Explicitly carves out foreign intelligence surveillance operations from the criminal procedure protections of ECPA, thereby further clarifying that these types of operations are governed exclusively by FISA.

Section 206

This affects the roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978. This amendment will result in increased roving tap activity. In particular, it expands FISA court orders to allow "roving" surveillance in a manner similar to ECPA wiretaps. The federal wiretap statute, but not FISA, was amended 15 years ago to allow, "roving taps." A roving wiretap enables government investigators to intercept all of a suspect's wire or electronic communications relating to the conduct under investigation, regardless of the suspect's location when communicating. The quintessential situation requiring a roving wiretap in the past has been when a suspect goes from phone booth to phone booth numerous times in an effort to prevent his calls from being wiretapped. Since September 11, 2001, the Administration has cited surveillance challenges posed by "disposable" cell phone situations where a suspect buys a cell phone on day one and a week later buys another cell phone with another number and moves from cell phone to cell phone seeking to avoid interception. But "roving tap" authority is not limited to voice communications; it could equally be used to intercept the email communications of a suspect who changes Internet accounts every day, or several times a day.

Section 209

This allows seizure of voice mail messages pursuant to warrants. Stored voice mail will be treated as stored data under and not as an intercept governed by wiretap procedures. This section enables law enforcement to seize voice mail messages via a search warrant, instead of a Title III wiretap order, which harmonizes the manner in which both voice mail and email messages can be accessed. It thereby overturns case law that requires the government to apply for a Title III warrant before it can obtain unopened voice mail messages (but not email messages) held by a service provider.

Section 210

This increases the scope of gaining subpoenas for records of electronic communications. This may produce a major increase in subpoenas regarding subscribers. This broadens the types of subscriber records that law enforcement can obtain via subpoena from service providers, including ISPs, to include "the means or sources of payment for such services," "records of session times and durations," and "any temporarily assigned network address." The means-of-payment category was broader earlier in the legislative process, but was subsequently narrowed to clarify that it encompasses credit card or bank account number used as a means of payment for the communication service. Therefore, this provision does not apply to payment information that is stored briefly on a service provider's system or information contained in a "digital wallet."

Section 211

This is a clarification of scope and changes procedures that apply to cable operators responding to a subpoena, and in most instances it will eliminate any obligations to notify customers of cable-based Internet service. This clarifies that ECPA governs the release of most subscriber records of cable television companies that provide Internet service. It will provide certainty to cable-based ISPs when served with lawful surveillance requests. Fixing a drafting flaw in the Administration's original proposal, Section 211 will result in cable operators responding to law enforcement requests by producing customer data about Internet service subscribers without first having to notify the subscribers. This is consistent with recent court decisions ruling that ECPA must have implicitly repealed a conflicting Cable Act requirement that subscribers receive advance notice of the government's request. One category of Internet subscriber information that still remains subject to the advance notice provisions of the Cable Act is "records revealing cable subscriber selection of video programming from a cable operator."

Section 212

This section grants emergency disclosure of electronic communications to protect life and limb. This expands the flexibility to disclose information in emergencies. This will permit service providers to disclose the content of stored email messages and other customer information whenever the provider "reasonably believes" that an emergency involving immediate danger of "death or serious physical injury to any person" requires such

disclosure. There was no provision in existing law expressly permitting service providers to make such emergency disclosures. This section should help resolve an ambiguity in current law that inhibits service providers from disclosing customer information in emergency situations involving death or serious physical injury.

Section 214

The expansion of pen register and trap-and-trace authority in FISA should lead to a significant increase in such requests for these tools. This will make it easier for the government to obtain a court order under FISA for pen register or trap-and-trace surveillance. Eliminates the requirement that the government certify that it has reason to believe that the surveillance is being conducted on a line or device that is or was used in "communications with" someone involved in international terrorism or intelligence activities that may violate U.S. criminal law, or a foreign power or its agent whose communication is believed to concern terrorism or intelligence activities that violate U.S. law. Instead, this section makes the FISA pen register and trap-and-trace requirements more closely track ECPA's requirements for such surveillance, e.g., by providing a certification that the information obtained would be relevant to an ongoing investigation. However, this section clarifies that a FISA court order should not authorize the gathering of foreign intelligence information for an investigation concerning a U.S. person or surveillance where the person has been singled out for investigation "solely upon the basis of" First Amendment activities.

Section 215

This section provides additional access to records and other items under the Foreign Intelligence Surveillance Act (FISA). Potentially a broad expansion of the types of items that may be subject to FISA subpoena; may include servers, but provides for immunity for good faith disclosures. This provision substantially revises the FISA provisions governing access to business records for foreign intelligence and international terrorism investigations. Most significantly, the provision no longer limits the FBI's ability to obtain business records pursuant to a court order to specific categories of businesses. Previously, section 501 of FISA had subjected only common carriers, public accommodation facilities, physical storage facilities, or car rental facilities to FISA business record authority. By eliminating these categories and allowing these subpoenas to be issued to any person, Congress has, for example, included Internet service providers, libraries, banks, and any other business within the reach of business record authority. Second, Section 215 creates immunity for good faith disclosures of business records under this provision, and provides that disclosure of records does not waive any privilege in any other proceeding or context. Third, Section 215 eliminates a previous limitation of FISA business record authority to "a foreign power or an agent of foreign power," and expands the scope of items that may be obtained through this authority from "records" to "any tangible things," which might include, for example, a computer server on which information is stored. Fourth, the provision specifically prohibits investigations under this authority of U.S. persons that are conducted solely based on First Amendment activities. Finally, this section requires the Attorney General to fully inform and provide reports to select congressional committees, on a semiannual basis, of all requests for production of "tangible things," and to indicate in his report the total number of

applications made, in the preceding six-month period, for court orders and, of those, the number of applications that were granted, modified, or denied.

Section 216

This is the most significant surveillance expansion in the Act that deals with the modification of authorities relating to the use of pen registers and trap-and-trace devices. This section clarifies that pen register, and trap-and-trace authority applies to Internet traffic, permits nationwide service of process, and requires reports on use of "Carnivore"type technology. There are three major changes to existing law. First, by adding the terms "routing" and "addressing" to the phrase "dialing and signaling information," this amendment is intended to clarify that the pen register and trap-and-trace authority under ECPA applies to Internet traffic, provided that the information retrieved by these devices "shall not include the contents of any communication." Although the term "content" has a statutory definition, it is vague and has not been tested in the context of Internet communications. The term content "includes any information concerning the substance, purport, or meaning of the communication." It will be important to monitor law enforcement requests to determine what Internet-related information law enforcement seeks to obtain under the new law beyond the "to" and "from" header information in email communications that it already receives under existing pen register and trap-andtrace law. Second, this provision also grants federal courts the authority to issue pen register and trap-and-trace orders that are valid anywhere in the United States, not just within their own jurisdiction. The advent of nationwide service will likely result in providers being asked with some frequency to render assistance even though they are not specifically named in the order and the assistance being requested is not specifically defined in the order. This section provides that a service provider has the right to receive a written certification from law enforcement confirming that the order applies to the provider being served with it. Moreover, this section clarifies that compliance with a pen register and trap-and-trace "order," rather than the express "terms of such order" makes a service provider eligible for statutory immunity. Nevertheless, nationwide service could make it very difficult for local or regional service providers to oppose, modify, or contest court orders because it will require service providers to travel to numerous courts, in multiple jurisdictions, to address concerns over the breadth of court orders. Third, Section 216 directs law enforcement to file an *ex parte* and in camera report with the court whenever it uses a "Carnivore" device (defined as "installing and using its own pen register or trap-and-trace device on a packet-switched network" of a provider). The report would identify, *inter alia*, "the configuration of the device at the time of its installation" and "any information which has been collected by the device." The existence of these reports may help in future public policy debates on the propriety of the government compelling ISPs to install "Carnivore" devices and the extent of the use of such devices. This provision is a permanent change to federal law and is exempted from the sunset provision of Section 224.

Section 217

This provision deals with the interception of computer trespasser communications. It protects the government from liability for warrantless interceptions of hackers and similar "trespassers" (persons who are not known to owner or operator of the computer to have a

contractual relationship with that owner or operator and who gain unauthorized access to the system) at the request of a service provider. This section provides new protection from liability for government officials if they conduct warrantless wiretaps of computer "trespassers". The drafters presume that, under the "switchboard" provision of existing law, owners or operators of computers have the authority to intercept the communications of trespassers. This section is designed to protect law enforcement officials when the owner or operator delegates that authority to law enforcement. Under the "switchboard" exception, a service provider can intercept or disclose a user's communications when "necessary . . . to the protection of the right or property of the provider." Although the House Judiciary Committee bill contained language that would have explicitly protected the service provider from liability for authorizing or providing facilities or technical assistance for this surveillance, the final legislation does not contain this language. To the extent that a court determines that the "switchboard" exception does not authorize owners or operators of computers to intercept the communications of trespassers, this omission could present a problem because there is case law indicating that ECPA's good faith defenses are not a basis for avoiding liability where actions are taken on the basis of an erroneous belief that a statutory provision authorizes the action. Nevertheless, Section 217 does not compel service providers to permit law enforcement to engage in the warrantless surveillance of trespassers, but rather leaves that decision entirely to the discretion of the service provider.

Section 218

This relaxes the standards for FISA surveillance in regards to foreign intelligence information requirements for FISA authority. This provision amends FISA to require a certification that "a significant purpose," rather than "the purpose," of surveillance or search under FISA is to obtain foreign intelligence information.

Section 219

This creates single-jurisdiction search warrants for terrorism that greatly facilitates nationwide warrants for terrorism investigations. This provision amends the Federal Rules of Criminal Procedure to allow federal judges to issue nationwide search warrants for investigations involving domestic or international terrorism. Now federal magistrate judges may issue search warrants in any jurisdiction where activities related to terrorism may have occurred for a search of property or for a person within or outside the district. It will be much more difficult to seek review of orders that are issued remotely. To the extent that this modification makes government investigations easier, providers can expect to see an increased volume of requests. Also, the government in some instances will be able to choose a forum that is more likely to approve its requests.

Section 220

This provides for expanded nationwide service of search warrants for electronic evidence. This provision amends ECPA to allow a single court having jurisdiction over the offense to issue a search warrant for stored data such as email that would be valid anywhere in the U.S. To the extent that this modification makes government investigations easier, providers can expect to see an increase in volume of requests for assistance.

Section 222

This provides assistance to law enforcement agencies. This critical provision makes it clear that the Act does not affect, either positively or negatively, the ability of the government to require technical mandates. This makes clear that the legislation preserves the *status quo* with regard to technical mandates and other obligations on service providers to provide technical assistance to law enforcement. The language recognizes technical mandates in other areas (namely CALEA, which applies to telecommunications services, but generally does not apply to the Internet), while at the same time making clear that the Act does not require ISPs to reconfigure their systems in any way to allow the interception of or storage of Internet Protocol traffic.

Section 223

This grants civil liability for certain unauthorized disclosures that provide somewhat greater accountability of government agents for willful unauthorized disclosures of fruits of wiretaps and production of stored data. This provision makes a number of changes to prohibitions against unauthorized disclosure by the government of information obtained through the surveillance authority provided by ECPA. The most significant of these changes is an explicit clarification that civil lawsuits are not available against the federal government for unauthorized interceptions or disclosures. However, it does not preclude actions against government agents, specifically prohibits willful unauthorized disclosure or use of information that the government obtains through surveillance, and increases the accountability of the government to discipline employees who willfully violate these sections. The end result is nonetheless more favorable to the government.

Section 224

This Act has a four-year sunset for many relevant sections. This mainly sunsets the surveillance and intelligence gathering provisions (all of Title I and Title II) of the bill. The list of exceptions not covered by the sunset is as follows:

- Section 203 broadening the authority to share grand jury information.
- Section 203 establishment of procedures regarding the sharing of criminal investigative information.
- Section 205 expedition of employment of translators to support counter terrorism.
- Section 208 designation of FISA judges.
- Section 210 broadening the scope of subpoenas for electronic communications service providers by requiring disclosure of the means and source of payment, including bank account or credit card numbers.
- Section 211 treating cable companies that provide Internet services the same as other ISPs and telephone companies for such services.
- Section 213 broadening the authority to delay notification of search warrants in criminal investigations if prior notice would have an adverse effect.
- Section 216 extending trap and trace to Internet traffic so long as excludes "content."
- Section 219 single-jurisdiction search warrants for terrorism.
- Section 221 trade sanction amendments.

• Section 222 - no imposition of technical obligations on provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance.

Section 225

This grants immunity for compliance with FISA wiretap, which is a very important expansion of service provider immunity for compliance with FISA. This section provides immunity for civil liability from subscribers, tenants, etc. for entities that comply with FISA wiretap orders. This creates complete immunity for providing "any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under FISA. Previously, FISA had failed to include protection for complying with FISA wiretaps. Section 225's liability protection is important because FISA wiretaps are likely to increase.

Section 326

Companies, especially financial institutions like Banks and Credit Unions, need to know whom they are doing business with. According to this section, financial institutions will be required to implement reasonable procedures for:

1. Verifying the identity of any person seeking to open an account, to the extent reasonable and practicable.

2. Maintaining records of the information used to verify the person's identity, including name, address and other identifying information.

3. Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

4. Each financial institution must comply with this final rule by October 1, 2003.

An account is defined as a formal relationship to provide or engage in services, dealings or other financial transactions:

Includes:

- Cash management
- Credit accounts and other extensions
- Custodian services
- Transaction or asset accounts
- Trust services

Excludes:

• A product or service without a "formal" relationship, i.e., check cashing, wire transfer, sale of a money order

• Acquired accounts via acquisition, merger, asset purchases, liability assumption

A customer is a person opening a new account and/or an individual who opens a new account for one who lacks legal capacity (e.g., a minor) or an entity that is not a legal person (i.e., a civic group)

Excludes:

- A person with an existing account, provided identity is "reasonably" known (How is this determined??)
- Other domestic operated financial institutions, government agencies, or publicly traded companies

This area is getting particular attention because it helps with examining money flowing in and out of accounts and ensuring adherence to know-your-customer rules, which are thematic throughout the Patriot Act.

Section 351-361

These are the Bank Secrecy Act amendments and related improvements. The main point is the expansion of the Bank Secrecy Act in connection with bank records. These sections generally amend the law in ways that will permit increased government access to terrorism-related information from banks. At the same time, institutions and their directors, officers, employees, and agents are protected from liability for such reporting of suspicious banking activities. Similar provisions also apply to securities brokers and dealers regulated by the Securities and Exchange Act of 1934. Likewise, the Fair Credit Reporting Act is amended to allow consumer-reporting agencies to provide consumer reports to government agencies for counter terrorism purposes.

The provisions also require financial institutions to develop anti-money laundering programs. The banking provisions allow the Secretary of the Treasury to impose sanctions, including cutting off all dealings with United States financial institutions, on banks in a nation whose bank secrecy laws deny information to the Federal Bureau of Investigation or other agencies. Foreign banks maintaining correspondent accounts in United States banks must designate someone in the United States to receive subpoenas related to those accounts and their depositors. If those subpoenas are not answered, the accounts could be ordered closed. These amendments also bar United States banks from doing business with "shell banks" overseas: those operations that have no physical facilities and are not part of a regulated banking system. In addition, they empower the Treasury Secretary to require United States banks to exercise enhanced "due diligence" to find out who their private banking depositors are if they come from nations that will not assist United States officials.

Section 414

This section promotes visa integrity and security. It also expresses the sense of the Congress that the Attorney General, in consultation with the Secretary of State, should fully implement the entry/exit system as expeditiously as practicable. Particular focus

should be given to the utilization of biometric technology and the development of tamper-resistant documents. (Leahy)

Section 503

This authorizes the collection of DNA identification of terrorists and other violent offenders. Both the House and Senate bills included this provision to authorize the collection of DNA samples from any person convicted of certain terrorism-related offenses and other crimes of violence, for inclusion in the national DNA database. (Leahy)

Section 507

Amends the Family Educational Rights and Privacy Act (FERPA) to allow educational institutions to disclose educational records without court order or student consent when relevant to a terrorism investigation. The institution is not liable for disclosures made in good faith and need not retain a record of the transaction. FERPA already contained an emergency provision allowing for such disclosure if "necessary to protect the health and safety of the student or other persons."

Section 701

Expansion of regional information sharing system to facilitate Federal-State-local law enforcement response related to terrorist attacks. Both the House and Senate bills included this provision to expand the Department of Justice Regional Information Sharing Systems (RISS) Program to facilitate information sharing among Federal, State and local law enforcement agencies to investigate and prosecute terrorist conspiracies and activities and doubles its authorized funding for FY2002 and FY2003. Currently, 5,700 Federal, State and local law enforcement agencies participate in the RISS Program. It also calls for the establishment of a secure information sharing system. (Leahy)

Section 808

Provides the definitions for the Federal crime of terrorism. Both the House and Senate bills included this provision to update the list of predicate offenses under the current definition of Federal crime of terrorism. Adds certain computer fraud and abuse offenses to the list of violations that may constitute a Federal crime of terrorism.

Section 814

The deterrence and prevention of cyber-terrorism expands government's authority to prosecute hacking, and denial of service attacks creates provisions for private litigation under the Computer Fraud and Abuse Act, clarifies the meaning of damage/loss under the CFAA, and precludes private lawsuits for negligent design or manufacture of hardware or software. This section increases criminal penalties for Computer Fraud and Abuse Act (CFAA) violations, adds computers located outside the U.S. to the definition of "protected computers" covered by the statute, adds a definition for the important, but previously undefined, statutory term "loss," and clarifies that criminal prosecutions for hacking or unauthorized transmissions may be brought against the accused if a "related course of conduct" causes \$5,000 in loss. At the same time, Section 814 contains several improvements upon current law for civil defendants, who have increasingly become a

target of plaintiff class actions brought using the private right of action contained in the CFAA.

First, it provides that the CFAA \$5,000 damage threshold is satisfied through loss caused by a related course of conduct "for purposes of an investigation, prosecution, or other proceeding brought by the United States only." The negative implication of this language appears to be that a single act, not a related course of conduct, producing \$5,000 in harm is necessary for anyone other than the government to bring a private lawsuit under the CFAA. Second, it generally preserves the current \$5,000 threshold for private lawsuits under the CFAA for "loss" to a computer system, except for cases involving damage to a system used by the government for the administration of justice, national defense, or national security. It also clarifies that the \$5,000 threshold required for a private lawsuit applies both to actions for "damage" and "loss," thereby eliminating a statutory ambiguity that plaintiffs' class action lawyers had attempted to use to avoid the \$5,000 threshold. Third, it contains a provision from the original Senate bill stating that "no action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." Although this language could be clearer, this provision likely will be very helpful in obtaining dismissal of CFAA class action claims such as those challenging alleged defects in software or hardware.

Section 815

This section provides an additional defense to civil actions relating to preserving records in response to government requests. This expands businesses defense in civil actions alleging disclosure to governments. This section adds a new defense to civil or criminal liability under ECPA for companies who preserve stored data at the request of a law enforcement official.

Section 816

Provides for the development and support of cyber security forensic capabilities. Both the House and Senate bills included this provision to require the Attorney General to establish regional computer forensic laboratories and to support existing computer forensic laboratories to help combat computer crime.

Section 1001

Directs the Office of the Inspector General (OIG) in the U.S. Department of Justice (DOJ) to undertake a series of actions related to claims of civil rights or civil liberties violations allegedly committed by DOJ employees. It also requires the OIG to provide semiannual reports to Congress on the implementation of the OIG's responsibilities under Section 1001. [USDOJ – OIG]

Section 1009

This provision directs the FBI to report to Congress on the feasibility of providing airlines with computer access to the names of suspected terrorists. (Leahy)

Section 1016

Deals with critical infrastructures protection. This provision establishes a National Infrastructure Simulation and Analysis Center (NISAC) to address critical infrastructure protection and continuity through support for activities related to counter terrorism, threat assessment, and risk mitigation.

Appendix B – Information Technology Aspects of Patriot II

On February 7th, 2003, a draft of a Federal Government bill entitled the "Domestic Security Enhancement Act" was leaked to the public. The purpose of this draft would be to enhance and expound on the Patriot Act and has therefore frequently referred to by the nickname "Patriot II". Since this draft has not yet been formally introduced to the Senate or House for voting and has been met with considerable controversy, it may not actually ever come into existence. Therefore, the purpose of this section is merely to describe the sections of the draft that are relevant to information technology.

Section 107

Under the current Patriot Act, the use of pen registers for U.S. people is stricter than for non-residents. Using these devices for non-residents must be done to "obtain foreign intelligence information"; while, for U.S. residents, the registers may only be used to "to protect against international terrorism or clandestine intelligence activities". Section 107 of Patriot II reduces the U.S. resident standard to the "obtain foreign intelligence information" standard of the non-resident. [26]

From an information technology perspective, this section would enable the government to obtain Internet usage information from American citizens if necessary to "obtain foreign intelligence information". Such usage information could include Internet sites visited and sent or received email addresses. Obviously, this would increase the existing Patriot Act data storage burden on ISPs. Also, companies whose employees use email and/or the Internet could conceivably be expected retain such usage information on their employees for a certain minimum length of time. [8]

Section 124

This section addresses the monitoring of multifunction devices. Currently, the laws in place are vague on whether it is legal, when monitoring a multifunction device for a specific function, to also monitor the other functions of the device. For example, many modern cellular phones also have an Internet browser available. Current law is unclear on whether, while monitoring phone calls on a particular cell phone, it is legal to also monitor the websites visited from that same phone. Section 124 would eliminate this ambiguity, making it indeed legal to monitor all functions within a particular multifunction device. [26]

This part of the new law, if in existence, would likely compel manufacturers and/or service providers on multifunction devices to expand their scope of data storage and availability. For instance, a cell phone company that has had to provide phone usage records would also have make available and accessible information pertaining to websites visited, emails sent, and other functions it may provide.

Sections 128 and 129

Section 128 of Patriot II involves "administrative subpoenas", which are subpoenas that Federal law enforcement may obtain without the consent of a grand jury. This type of subpoena may currently be used to enhance the investigation of a wide variety of Federal crimes, but not terrorism, which is perhaps more heinous than any of the other crimes for which these subpoenas may be used. Therefore, section 128 would render the use of administrative subpoenas legal in terrorism investigations. (Daily Rotten)

Section 129 pertains to a type of administrative subpoena called a "national security letter". These letters are used to aid Federal law enforcement to expedite the receiving of certain types of information, including "electronic communication transactional records maintained by communication service providers". This section is designed to eliminate some current shortcomings regarding national security letters. First of all, although current law prohibits the subjects of these letters from disclosing the fact that they were subpoenaed, there is no provision for penalizing those who do disclose such information. Section 129 would specify a specific punishment for such violations. Also, while recipients of these subpoenas are currently under legal obligation to provide the requested information, no means of enforcing this currently exists. Section 129 would rectify this situation as well. This section would also expand the current scope of national security letters so that they pertain to domestic as well as international terrorism. Finally, Section 129 would also clarify existing laws regarding the sharing of national security letter information among Federal agencies. (Daily Rotten)

These sections, as they pertain to communication service providers, would further reiterate the need for ISPs, cell phone companies, and other providers of electronic communication providers retain usage information and make it readily accessible. In addition, these sections would reemphasize the need for these providers to remain confidential in providing the Federal government with requested information.

Section 404

This section proposes to address the issue terrorists and other criminals using cryptography to send emails and other data to assist them in carrying out their crimes. Existing laws do not prohibit the use of encryption to help plan out or execute a crime. Section 404 would in fact make such use of encryption illegal. In addition, this section would set in place a punishment for these abusive uses of encryption of at least five years imprisonment added on to the prison sentence for the crime itself. (Daily Rotten)

If Patriot II were to become law, this section would foster information technology repercussions in both the public and private sectors. First, the Federal government would have to increase its already considerable investment in information technological resources to become more adept at intercepting and decrypting transmissions possibly related to terrorism or other crimes. Within the private sector, ISPs and encryption technology manufacturers would have to potentially make encryption keys available to Federal law enforcement in certain instances.

<u>Title III, Subtitle A</u>

From an information technology perspective, this component of Patriot II is by far the most compelling piece of this proposed legislation. Subtitle A involves the creation of a "Terrorism Identification Database". This subtitle is composed of sections 301 through 306. Section 301 relates merely to the title, so Sections 302 through 306 are discussed below. (Daily Rotten)

Section 302

Currently, Federal law enforcement may collect the DNA of those who commit certain crimes, terrorism not being one of these crimes. Section 302 would enable law enforcement to collect DNA samples and other information regarding suspected terrorists. (Daily Rotten)

Section 303

This section would provide for the creation of databases of terrorist or suspected terrorist DNA records and other vital information. All Federal agencies would be required to give to the Attorney General any relevant DNA records they have collected for inclusion in the database. In addition, Section 303 would grant the Attorney General the use of this database in investigating, prosecuting, and otherwise fighting terrorism. Finally this section would allow the Attorney General to share the data with Federal, State, local, or foreign agencies as needed for anti-terrorism purposes. (Daily Rotten)

Section 304

This section provides for definitions of the terms "DNA sample", "DNA analysis", and "suspected terrorist". (Daily Rotten)

Section 305

This section provides for the creation of new authorities as needed and stipulates that enforcement agencies will not preclude other laws pertaining to the use of DNA evidence. (Daily Rotten)

Section 306

This section would amend existing laws so that Subtitle A would apply even to terrorists who are paroled, conditionally released, or otherwise Federally supervised. (Daily Rotten)

Information Technology Impacts

The information technology impacts of Title III, Subtitle A would be considerable. First off, passage of this legislation would warrant the Federal government to design or outsource the design of a very large, flexible, state-of-the-art database to hold and

maintain the data. Such a database would also potentially require compatibility with State, local, and foreign agencies with which data may be shared as required for terrorism investigations. Costs to the government (and thereby the taxpayers) would be quite substantial.

Secondly, such a database may spurn off an entirely different wave of controversy. In addition to the ongoing controversy over privacy and constitutionality concerns of the Patriot Act and Patriot II, public outcry would quite likely ensue over the ethicality of maintaining such biological data. (Another group in this Capstone Course has written an in-depth paper on Bioinformatics.)

Appendix C

Author Information

Dr. Paul C. Jorgensen

Paul graduated with a B.A. in Mathematics from North Central College in 1964, an M.A. in Mathematics from the University of Illinois in 1965, and a Ph.D. in Computer Science from Arizona State University in 1985. He worked in various divisions of GTE Corp. 20 years, and then joined the faculty of Arizona State University for two years. He has been at Grand Valley State University since 1988, and is a full professor in the Computer Science and Information Systems department.

His teaching, research, and consulting interests coincide on models for requirements specification and software testing. He is the co-author of two books and the sole author of *Software Testing-A Craftsman's Approach*, 1st and 2nd editions. He is a Senior Member of IEEE Computer Society.

Jason Kadzban

Jason graduated from Grand Valley State University in 1993 with a degree in Communications. In 1996 he earned a second degree in Business Administration, and in 1998 he earned a third degree in Computer Information Systems, both form Aquinas College. He will graduate from Grand Valley State University in December 2003, with a Masters of Science in Computer Information Systems. Jason has worked as a Programmer, Systems Analyst, Network Administrator, DBA, and Project Manager at such companies as WOOD TV8, CCMS, and Progressive Distribution. Currently Jason works for Maximus, is married to wife Jannete, and has two small daughters – Isabelle and Hannah.

Samuel H. Gustafson

Sam received a Bachelors of Business Administration in Accountancy from Western Michigan University in April 1997. Also, Sam will graduate from Grand Valley State University in December 2003, with a Masters of Science in Computer Information Systems. Sam has worked in the accounting field as a financial/operational auditor in State government and in the retail industry. Currently, Sam works in the insurance industry as a programmer.

Donalyn K. Sandborn

Donalyn graduated with a Bachelors of Arts Degree with a Major in Elementary Education from Michigan State University in 1990. She taught for five years at a private school and then gained a teaching position at a Computer Learning Center. Thereafter, Bath Community Schools hired her as their Technology Coordinator. For the last six years, she has been the IT Manager at Portland Federal Credit Union where she has also run the VISA and ATM/Debit departments. Areas of strength are Project Management, Training, IT Security, and Network and Phone Administration. Donalyn will graduate with a Masters of Science in Computer Information Systems from Grand Valley State University in 2003.

Carol J. Capek

Carol earned a Bachelor of Business Administration, *cum laude*, in Finance from Western Michigan University in 1996. Carol will graduate with a Master of Science in Computer Information Systems from Grand Valley State University in 2003. Carol has worked in the Financial Industry for more than 22 years. Her experience is in Mortgage Servicing, Mortgage Technology, Project Management, and Technology Management. She is currently the Financial Systems Administrator for the City of Grand Rapids, Michigan.

Appendix D Assigned Sections.

Jason Kadzban:

Section II – Definition of the Issues Section III – Internet Service Providers Section IV – Data Mining

Samuel Gustafson:

Section III – Financial Institutions

Donalyn Sandborn:

Section IV - Overview of Business, Companies, Compliance, Foreign Country Needs, Consulting, Project Management, and Training

Carol Capek:

Section V – Government Impact

All:

Introduction and Conclusion