The US Patriot Act Deconstruction, Civil Liberties And Patriotism

Martin Carrigan, University of Findlay
Theodore Alex, Governor's State University
Chris Ward, University of Findlay

ABSTRACT

The US Patriot Act, passed after the devastating day of September 11, 2001, has dramatically affected all aspects of American daily activities. This paper examines its affect on organizational behavior.

INTRODUCTION

After the terrorist attacks on the United States on September 11, 2001, the United States felt a deep sense of vulnerability and need for improved national safety and security. In response to the ailing confidence and perceived failings of the government's ability to protect its citizens against terrorism, legislation was immediately introduced in the House of Representative to enhance domestic security against terrorism. This bill, H.R. 3162, became law only 45 days after its introduction on October 26, 2001 as Public Law 107-56 - The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, otherwise known as the Patriot Act. This law was designed to address the perceived failings in intelligence gathering and was designed to greatly modernize and expand intelligence and surveillance activities in the United States. In the process of addressing vital national security issues, however, the Patriot Act has changed the role of organizations to protect individual rights and meet the security needs of the government.

The original Patriot Act was valid only until 2005. After an extension was voted on and approved, on March 9, 2006, President Bush signed into law the updated and revised version. The updated version made most of the titles permanent with the exception of the authority to conduct "roving" surveillance under the Foreign Intelligence Surveillance Act and the authority to request production of business records under FISA, which are sections 206 and 215 of the act. Those acts will be up for revisions again in December of 2009.

PURPOSE OF THE ACT

The Patriot Act contains strong measures to prevent, detect and prosecute terrorism and international money laundering. The Act is far-reaching in scope, covering a broad range of financial activities, institutions and businesses. The Act was designed to protect US citizens from further terrorist attacks by making it harder for terrorists to launder the money they need to support their attacks, allow government agencies easier access to financial and personal information held by financial institutions, allow federal agents to ask a court for an order to obtain business records in national security terrorism cases and to allow government agencies to freely exchange information.

A spirited debate continues as to whether or not the Patriot Act has made America any safer. One group claims that since there has not been a terrorist attack on US soil anywhere like the Sept 11 attack, that the Patriot Act has been successful. Other groups have cried foul at the impact the Patriot Act has had on civil liberties and on how US business is now conducted.

As to its affect on organizations, many businesses have complained through their lobbyists that they now have to keep additional and costly paperwork on their customers, clients or employees. Businesses are also

concerned with how they will communicate to their customers, clients and employees the new regulations and how they impact their day by day activities. The Patriot act has changed the way that US business is conducted, and this paper will examine this affect on organizations.

THE ACT'S AFFECTS

When the Patriot Act was signed into law it amended at least 34 laws and/or regulations. Some of those laws and/or regulations are:

1. Title 18, United States Code (Crimes and Criminal Procedure)
2. International Power Act
3. Communications Act of 1934
4. Title 31, United States Code (Money and Finance)
5. Bank Holding Company Act of 1956
6. Bank Secrecy Act (Public Law 91-508)
7. Right to Financial Privacy Act of 1978
8. Fair Credit Reporting Act
9. National Security Act of 1947
10. Telemarketing and Consumer Fraud and Abuse Prevention Act
11. Crime Identification Technology Act of 1998 (Herold, 2004)

Virtually any business that handles personal information, provides connection to the Internet or does business internationally is impacted by the Patriot Act. In addition to the wide scope of businesses affected by the Patriot Act, the Patriot Act does dramatically affect the following types of businesses: financial institutions, international financial institutions, money transmitting businesses, and non-financial trade or business organizations.

AFFECT ON FINANCIAL INSTITUTIONS

Within the Patriot Act there are many controls, procedures and requirements that business are required to implement. Financial institutions must now designate one or more persons to receive information concerning, and to monitor accounts of, certain individuals and organizations and establish procedures for the protection of the shared information. One criticism to the changes to bank and financial institutions record keeping is that it will cost smaller institutions more time and money to update their systems to comply with the new rules. While smaller institutions may not have the technology available to immediately begin meeting these new requirements, large institutions are not automatically immune. Citigroup had to resort to using pen and paper to record additional customer identity information required under the Patriot Act when its computer system was not updated in time for the act's required implementation deadline (Martins, C. & Martins, S., 2005). In addition to updating their systems, smaller institutions may also have to hire and train additional employees to ensure they are adhering to these new requirements.

New Regulations applied by the Patriot Act have upped the ante in compliance for smaller institutions. In the past only large banking companies have used chief risk officers to keep track of all facets of risk – credit, rate, strategic, compliance, transaction, price, reputation, and liquidity. These chief risk officers are accountable and empowered to enforce new controls and procedures. They are required to communicate these new controls and procedures to all bank employees.

The Patriot Act has also affected the training given to bank tellers. Bank tellers must not only provide outstanding customer service to their customers and sell them additional bank services, but they also have to be properly trained by their managers to monitor for money-laundering activities. Banks must now communicate to their tellers how to monitor customer transactions and behavior, and make note of it if it varies from their normal activities. They must also be trained on how to check their customers against a list of potential terrorists or people allegedly involved in drug trafficking and money laundering activities. This list is provide by the Office of Foreign Asset Control, and bank employees need to check the names of people that have made recent transactions or open

accounts against those on the list. Most banks have purchased software that retrieves the list online and integrates it into their systems electronically (Paige, 2005). While one can buy software to run the checks, it is limited by the logical functions of the computer programmers. While the new security software can flag a large withdrawal or money transfer, it can not observe the actions of the person making the withdrawal or money transfer. Only a bank employee that has been trained to watch for certain behaviors or actions can detect them.

Banks have added new training techniques, such as e-mail alerts and online training modules to help their tellers keep up with their new responsibilities. Gone are the days when you could just hire a teller, give them a quick orientation and set them loose. Because of all the new regulations, banks must now spend time constantly training and communicating with their tellers.

In addition to training their employees, banks are now faced with changing how they interact with their customers. With new homeland security rules required by the Patriot Act, banks and credit unions are facing increased security requirements. While banks and credit unions have required identification from customers in the past when opening an account, they must now document this information. The new regulations now require four pieces of information on new and existing account holders: name, physical address, identification number, which for U.S. citizens is their Social Security Number, and date of birth. All the information must be verified.

Most customers seem to understand that the requirements are in place for a good reason, according to Ed Aycock, senior vice president and regulatory counsel with the North Carolina Bankers Association (Paige, 2005). Many banks and credit unions are now keeping literature in their lobbies designed to educated customers on the Patriot Act and how it affects financial institutions. Much of the literature focuses on explaining that the identification requirement the bank or credit union is imposing on their customers is required under federal law.

Most bank officials acknowledge that one of the biggest changes and challenges that they now face because of the Patriot Act is how to communicate to their organizations the types of transactions that must be reported to the government.

Financial institutions must also run background checks on anyone applying for financing. The Treasury Department's Office of Foreign Asset Control maintains the "specifically designated nationals" (SDN) list of people blocked from participating in 'any transaction or dealing…in property or interests' within the United States. These people have been identified 'to have committed, or to pose a significant risk of committing, acts of terrorism'. Although the blocked-persons list has been around in some form or other for nearly a decade, under The Patriot Act, private individuals such as jewelers, pawnbrokers and home buyers and now considered by the government to be financial institutions.

While many business leaders felt the burden of their newly gained "detective" status, the burden seemed to weigh more on banking organizations. Banks were required to conduct an investigation on their employees and they were also responsible for conducting full background checks on each and every person applying for financing. After the passing of the Patriot Act, bank executives were mandated to run checks on all potential clients using a Federal Internet database system that listed the names of individuals suspected of being involved in terrorist activity. Bankers were also expected to more highly monitor their check cashing services. The Patriot Act also greatly limited the freedoms banks had to do business with foreign banks.

The Patriot Act prohibits banks from establishing, maintaining, administering, or managing a correspondent account in the U.S. for a foreign shell bank. Banks are also required to take reasonable steps to ensure that any correspondent account the bank maintains with a foreign bank is not being used to indirectly provide banking services to a foreign shell bank. Additionally, banks that maintain a correspondent account in the U.S. for a foreign bank must maintain records identifying the owner of the foreign bank and the name and address of a person residing in the U.S. who is authorized to accept legal service of process. (Podzolka & Deberry, 2003, p. 63)

The burden to check these names against the list has now fallen to the title companies. Because the SDN list is a public document, initially many title agencies do not charge for this search (Braiker, 2004). However, more

and more companies are beginning to charge for the search to cover the time it takes to conduct the search and the training they must give their employees to do the search and than record the information per government regulations.

AFFECT ON CABLE/TELECOMMUNICATIONS INDUSTRY

The cable industry has also been impacted by new records retention requirements under the Patriot Act. Cable companies that offer Internet services, in particular, have had to change recordkeeping practices in order to comply with the new standards. This is principally because of differences in the way that requests for cable TV subscriber versus CABLE Internet subscriber information requests are handled under the Patriot Act. The amount and type of information required to be provided is much greater for Internet subscriber data than for cable TV subscriber information (Martin, C. & Martin, S., 2005). Keeping these two separate has become a challenge for record management managers. In addition to adjusting how they retain their records, some businesses have had to add on more employees to keep up with the information requests coming from the government.

The records retention requirements that are now required under The Patriot Act has not only caused businesses to add more employees and to spend more money on training, but some businesses have had to develop entirely new departments to adhere to these changes. Some times these compliance groups work well with the existing records management groups and sometimes not. Corporate culture and the function of the groups involved are influential factors in applying any new law to an existing records management program.

Existing records policies and systems must be analyzed in light of these new requirements. The documentation of the analysis and any changes to a businesses current records management policy should be as detailed as possible and communicated to all parties involved.

AFFECT ON STRUCTURE

The Patriot Act has also affected the way organizations are constructing new offices and floor plans. The American Society of Interior Designers released a report linking the heightened emphasis on privacy to new laws such as the Patriot Act (Pulley, 2006). With more companies opting for close-packed, open work stations, privacy has become a major issue in the modern office. Workers complain about the lack of it and they seek creative solutions to dealing with the problem.

Organizations are looking to construct new offices that balance the need for teamwork and the desire for privacy. Valerie Hoffman, director of interior design for Lionakis Beaumont, states that you have to know who your client is to know how sensitive their documents are (Pulley, 2006). The open-plan office probably will not work for attorneys, doctors, bankers, accountants and other professionals who must deal with the kinds of sensitive client information protected by the Patriot Act, but could be effective for other professions.

Many organizations are opting for the best of both worlds, an open inviting floor plan with opportunity for both easy interaction and strict privacy when needed. To increase work productivity, while at the same time ensuring privacy, organizations are moving towards private pods and huddle rooms. These new office designs incorporate liberal doses of natural light and include open pods for team members. Higher partitions are erected around the perimeter of each pod to provide visual privacy, block sound from nearby workstations, and minimize distractions from passing workers in the aisles. Flat plasma computer screens can be mounted on moveable arms that can be positioned to prevent other workers or clients from viewing sensitive data. Huddle rooms provide employees and their managers an area to have private conversations when necessary. Organizations are also including special conference rooms in their floor plans to allow for private meetings with clients away from the desks, where sensitive data may be visible.

Organizations have seen an increase in productivity after moving into a more open, but at the same time secure office space. Dennis McConnell, Nolte Associates chief information officer, has indicated that his company has seen a 5 percent increase in billable hours (Pulley, 2006).

AFFECT ON INTRA-COMPANY COMMUNICATION

The Patriot Act has also impacted how, and by whom, communication within an organization can be monitored. The Patriot Act vastly expanded the authority of law enforcement to monitor private communication and personal information. Employers, on the other hand, must be careful when monitoring employee communications or divulging personal information. Most employers can avoid privacy claims by giving written notice and getting employees' written consent to monitor. Many employers are amending their policies to state they will cooperate with requests from law enforcement for access to employee files (Wilson, 2002).

AFFECT ON LIBRARIES

Also affected by the Patriot Act were United States libraries and their patrons. "The national Library Research Center did a poll in 2002—well before the librarians began their protest—and found that federal agents had requested information on patrons under the PATRIOT Act in sixty libraries. In May 2003 Viet Dinh himself admitted to the House Judiciary Committee that libraries had been contacted approximately fifty times in 2002 using the PATRIOT Act." (Tiefer, 2004, p. 87) It has been stated that this act had enabled the Federal Bureau of Investigation to obtain library records from any individual without showing any evidence of terrorist related activities. Furthermore, if asked to provide such information, librarians would be forbidden from informing customers that they have released this information. "Such is the state of affairs that librarians across the country are putting up signs warning patrons that the FBI may be snooping among their records." (Sanders, 2003) The American Library Association has encouraged all librarians and library administrators to inform their patrons, staff and communities about the process for compliance with the United States Patriot Act. As I checked out the book from which I just quoted, I was asked to sign a waiver. It stated that I understood the possibility of my records being released to the United States government…proof that the Patriot Act is still strictly enforced to this day.

It has been argued that the Patriot Act has taken away the right to read what one wants and when one wants with out the constant "peek over our shoulder". Some have gone as far as to argue that their First Amendment rights have been violated. While it has induced a "big brother" effect for some, many would claim that its statutes have been quite beneficial in the library arena. An example of this occurred in 2001 when an employee of the National Reconnaissance Office utilized public libraries to locate information on false identities and to schedule visits to foreign embassies. Brian Regan was eventually arrested for trying to sell national security secrets. This arrest was made possible through library investigations. ("Retired Air Force Sergeant," 2003, p. A03) (Kranich, N., 2006). Local librarians are working to minimize monitoring of library use by adopting privacy policies based on a model recently drafted by the American Library Association, destroying personally identifiable information not needed to administer services, and educating the public about problems with the law.

According to Joan E. Bernstein you should take nothing for granted when it comes to preparing ones staff to perform appropriately as protectors of customer privacy and confidentiality. If you want your employees to know something, make sure you communicate it to them in many ways and many times. Once you are confident they know and understand your message, communicate it to them again (Bernstein, J., 2007).

The issue of privacy of automated library records can affect everyone from patrons and library personal to the library board of trustees and township or city officials. To begin, libraries must be sure they know and understand the laws and regulations associated with The Patriot Act that affect them. Many libraries have retained a lawyer who has been directly involved in First Amendment issues. Once the library director and board of trustees understand the law, they must develop and put in place a privacy policy that is in compliance with applicable laws.

Every staff member should than be trained on the new policy and what they should do if law enforcement personal request confidential library records. This training should include some background information about the Bill of Rights, the USA Patriot Act, and state privacy protection laws (Bernstein, 2007).

Libraries are also facing the issue of what records they have to retain and for how long they have to retain them, and what records they can destroy. A policy addressing the disposition of both paper and electronic data

should describe what records your library retains and for what length of time. As a good rule of thumb, Bernstein suggest, that the less you retain, the less you have to worry about. There is nothing illegal or unethical about destroying or deleting records in a manner that is consistent with an established and documented record retention policy.

While there are many people libraries need to educate when it comes to their policies to protect the privacy of their patrons, none are more important than their employees. Libraries must be sure to over communicate and continuously train their employees to ensure that they will act confidently if they are ever approached by law enforcement personal seeking confidential library records.

BACKGROUND CHECKS

Safety and security measures for employees have been affected by the Patriot Act as well. Background checks have come under increased scrutiny. Many background checks are not being conducted properly, and some races and religions are being singled out. Employers who use a third person or vendor to conduct any kind of investigation must comply with the notice and authorization requirements of the federal Fair Credit Reporting Act that was amended by the signing of the Patriot Act.

AFFECT ON THE TRUCKING INDUSTRY

One specific industry that is finding itself impacted greatly by the Patriot Act is the trucking industry. Truckers who haul hazardous material are now required to undergo a security-threat assessment. The assessment is designed to track more closely the movement of hazardous materials. Drivers, who apply for, renew, or transfer a hazardous materials endorsement on their commercial driver license will undergo fingerprinting, background checks and an immigration check, according to the Department of Licensing. The hazardous materials endorsement and background checks are required for drivers transporting not only explosives, but also non-threatening commodities like paint, nail polish, chewing gum extract and soft drink syrup (Environmental NewsLink, 2005).

Speaking on behalf of the American Trucking Associations before a subcommittee of the U. S. House Committee on Homeland Security, Steve Russell, Chairman and Chief Executive Officer of Indianapolis truckload carrier Celadon Group, Inc. said that while the trucking industry supports the security objective, the current background check program has been marred by a number of bad decisions (Environmental NewsLink, 2005).

The costs to drivers and carriers are unacceptably high and serve as a disincentive to obtain a hazmat endorsement. The program has been implemented in a non-uniform manner across the states, has an insufficient number of fingerprinting locations, and limited hours of operation.

The trucking industry is currently facing a driver shortage of 20,000 long-haul drivers at a time when freight volumes are increasing. ATA members feel the background check provision will further exacerbate that shortage. By TSA's own estimate, the background check will result in a loss of 20 percent of the hazmat-endorsed driver population.

The trucking industry is not the only industry or profession being effected by the increased requirements and costs of background checks. Universities, trade schools, libraries, automobile dealers, real estate business, and flight schools are being impacted by the additional information now required for background checks and the additional costs associated with them.

As a result of the Patriot Act, flight schools are now required to closely scrutinize foreign nationals who come to the United States for flight lessons. The act requires that before foreign students can enroll in a flight school, they must seek permission from the U.S. Transportation Security Administration, which runs a comprehensive background check (Adams, 2005).

CRITICISMS OF THE ACT

The American Civil Liberties Union believes that the requirements on the financial institutions are one of many areas of redundancies being caused by The Patriot Act. According to Charlie Mitchell of the ACLU, 'Your money is already going to have been checked. You're going to have had the background checks at the banks. It's sort of emblematic of a lot of the Patriot Act. Some of the intentions are good, but there's just a casting too wide of a net to be particularly effective and there's a lot of unintended consequences when you do that' (Braiker, 2004). By compelling title companies to check out each party of a transaction, not only is the government passing on the cost of the war on terror to the consumer, they are requiring title companies to spend time and money training their employees to run background checks and maintain files that have already been completed by the banks involved in the transaction.

Some attorneys and watch groups find the Justice Departments power, given by the Patriot Act, to wiretap executive phones and bug boardrooms to investigate federal anti-trust crimes to be too broad. According to Philip Kircher, co-chair of the commercial litigation department at Cozen O'Connor, there is a possibility that the federal government will stick their noses into more routine business activity with the hope of finding minor violations (Swanton, 2006). Other concerns are that trade secrets and confidential strategy information will be made public and that attorney-client privilege could be breached.

REGULATIONS' IMPACT

More and more, business is being driven through regulation. Multiple regulations from Sarbanes-Oxley to HIPAA to The Patriot Act will continue to have a big impact on costs and how businesses communicate those changes to their employees, but will do nothing to increase revenue (Swanton, 2006) The question becomes how to minimize the impact on business operations.

What if your information and technology department had a single system that meets most regulatory requirements? What if you were able to determine that the processes, policies and procedures for many government regulations were very similar? For example, the way a life sciences company documents and certifies to the Food and Drug Administration that it cleaned its drug manufacturing tanks is similar to how a company might document and certify a change in procedures that affected revenue to meet Patriot Act requirements (Schwartz, 2006).

Most compliance software contains features that cut across most compliance issues; they include documentation, management, collaboration, process automation, and auditing. As requests for compliance software come in from different business units, only the IT department is in a position to see the commonality. The IT department must speak up and address the decision makers to integrate as many business units and the regulations and policies they must comply with into a limited number of software programs. Companies cannot afford to have point solutions for the DEA, DoJ, EPA, FDA, OSHA, and SEC, not to mention state and local requirements (Schwartz, 2006). As business is driven more and more by regulations, it is more critical than ever that business units and IT are aligned.

Businesses were expected to immediately comply with act although little or no explanation on the acts stipulations was provided. It was made known that companies were to investigate all of their employees regardless of their level in the said organization. While conducting these investigations, employers were to be looking for any connection of their employees with members of a comprehensive list of terrorists. Overall the productivity of many businesses declined due to the investigative commands that were now placed on the chief executive officer. Gaylen Knack, principal at the Minneapolis-based Gray Plant Mooty, voiced his frustration with the forced compliance of the Patriot Act by stating, "Congress adopted this broad business legislation in a short period of time and business leaders didn't fully understand what was being asked of them. Plus, some of these provisions might be impossible for companies to follow completely and for the government to monitor." Speaking of the investigative hassles specifically, he stated, "It is really impossible for companies with operations everywhere to constantly check this confusing list. Especially with how deep within these organizations we are being asked to look." (Martyka, 2002).

IMPACT ON THE JUDICIAL SYSTEM

The United States judicial community also felt a significant impact from the passing of the Patriot Act, most significantly in the arena of grand jury proceedings. "Section 203 of the USA Patriot Act amends Rule 6(e) of the Federal Rules of Criminal Procedure. Rule 6(e) codified a longstanding tradition of diligently preserving the secrecy of grand jury proceedings. Secrecy has been an important component of the grand jury process since at least the seventeenth century, when grand jurors successfully objected to the king's efforts to publicize--and thereby politicize--grand jury proceedings. This tradition of secrecy was incorporated by the American colonies into their own grand jury systems." (Collins, 2002) The United States courts have historically stated five main functions of Rule 6(e). These functions include preventing investigated defendants from potentially escaping; inhibiting these defendants from tampering with the investigation of other witnesses; preventing the said defendant from influencing the jurors themselves; providing public protection to those individuals who are later found to be innocent; and promising complete disclosure from grand jury witnesses. (Collins, 2002) Section 203 would have large reaching implications.

Section 203 dictated that the once highly secret information provided to the grand jury, must now be made readily available to federal law enforcement if this information involved matters of foreign intelligence or counterintelligence. As in all aspects of the Patriot Act, foreign intelligence related to any and all information which would signal a potential terrorist attack or similar danger to the United States. While Section 203 did discuss the "conditions' of this grand jury disclosure (informant may only use information in his official capacity, the extent of use may be limited according to established legal guidelines, and an attorney for the government must file that a disclosure was made to the court in a timely fashion), many members of the judicial community argued that these conditions were not stringent enough to protect the security of grand jury cases.

SUCCESSES OF THE PATRIOT ACT

The United States Patriot Act has proved successful on many fronts. This is found to be true even though some of the provisions of the act have "sunset" (no longer enforced) in 2005. It is believed that the men and women fighting for the freedom of our country today would not have the specialized equipment such as night-vision equipment and smart bombs which help them to defend and capture overseas. These words, spoken by John Ashcroft in an address to the United States Congress in Washington DC on July 13th, 2004, depict the magnitude of impact this act has had on the United States, "The Patriot Act is al Qaeda's worst nightmare when it comes to disrupting and disabling their operations here in America. Our law enforcement and intelligence teams have never before been so integrated and coordinated, and technologically – equipped, to target the twenty-first century threat of global terror." (Gerdes, 2005)

There have been many specific incidents in which the Patriot Act has proved to be successful. For instance, "the Patriot Act made possible the arrest and indictment of a father and son in Lodi, Calif., for lying to federal agents about the son's attendance at an al Qaeda terrorist training camp." ("Strong Patriot Act Required," 2005, p. B03) There are numerous other examples of the Act's success. The report said the act helped secure six guilty pleas from an al Qaeda "sleeper cell" in Lackawanna, N.Y.; allowed the surveillance of a reputed terror cell in Portland, Ore., resulting in convictions of six persons in a scheme to travel to Afghanistan to fight U.S. forces; and the successful prosecution of a money launderer for Colombia's leftist rebel group, the Revolutionary Armed Forces of Colombia, or FARC. It also credited the Patriot Act with the conviction of a man who sent more than 200 threatening letters laced with white powder to government agencies, businesses and individuals in Louisiana; and the discovery, through communication intercepts, of an 88-year-old Wisconsin woman who had been kidnapped and held for ransom. ("Patriot Act Chalks Up," 2004, p. A03)

Although the Patriot Act has offered the citizens of the United States protection in this age of terrorism, it has been argued by many that this security has come at a cost. That cost being the absence of one's civil liberty. This viewpoint is voiced quite clearly by the National League of Cities (NLC), one of the oldest and largest national organizations. The NLC and its supporters make it quite clear that they support the United States efforts to protect and defend against terrorism but at the same time do not believe that it should be done so by taken away the

guarantees promised in the Constitution. The NLC is in strong favor of amending the Patriot Act to protect the unalienable rights of the American citizen. There are others in favor of this also, "Those who, in effect, seek to suspend major parts of the Constitution and its Bill of Rights until we win the war against terrorism must realize that this is a long – term war and, hence, provisions that might apply for a very short period of time, during a dire state of emergency, cannot be applied here. To live for any length of time without the rule of law that makes us what we are is not an option, nor should it be." (Etzioni, 2004, p. 1) It's clear that the United States Patriot Act has had a profound effect on organizational behavior.

CONCLUSION

The Patriot Act has had a major impact on how business operate, communicate with, and train their employees. The added regulations have caused many businesses to revisit their policies on background checks, records retention and regulatory compliance software and to some extent, how they design their workspaces. The reality is that as long as The Patriot Act is on the books, it will impact businesses and businesses need to address it.

ABOUT THE AUTHORS

Martin Carrigan is an Associate Professor of Law and Business at the University of Findlay, and the Director of Business Administration. He received his BA degree from the University of Notre Dame, his MBA from the University of Findlay, and his JD from the University of Toledo.

Theodore Alex is an Associate Professor of Marketing at Governor's State University in Chicago, Illinois. He received his BSBA and MBA from Central Michigan University and his Ph.D. in Business Administration from the University of Arkansas.

Chris Ward is an Assistant Professor of Business at the University of Findlay, and the Director of Marketing. She received her BS and MBA from the University of Findlay and her Ed.D. from the University of Sarasota.

BIBLIOGRAPHY

1. Abdolian, L. F., & Takooshian, H. (2003). The USA PATRIOT Act: Civil Liberties, the Media, and Public Opinion. *Fordham Urban Law Journal, 30*(4), 1429+.
2. Adams, B. (2005, September 16). Patriot Act: Businesses cope with law's requirements. [Electronic Version]. *Business First of Louisville*
3. Bernstein, J. (2007, June). Train Employees and Officials to be Ready for Privacy Challenges. [Electronic Version]. *Computers in Libraries*, 7-8, 53-55.
4. Block, S., Waggoner, J. Chu, K. (2006). Insurers Required to Report Suspicious Activity. *USA Today*, B4.
5. Braiker, B. (2004, June 9). The 'Patriot' Search. *Newsweek News*. Retrieved July 16, 2007, from http://www.msnbc.msn.com/id/5131685/site/newsweek/from/ET
6. Breglio, N. K. (2003). Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance. *Yale Law Journal, 113*(1), 179+.
7. Chu, K. (2006). Watch Out: Your Mutual Fund Could Report You. *USA Today.*
8. Coats, B. (2002). Sufferable or Satisfying? Hard Policy Choices Within The USA Patriot Act of 2001. *Public Administration & Management: An Interactive Journal*. 7 (3), 211-228.
9. Collins, J. M. (2002). And the Walls Came Tumbling Down: Sharing Grand Jury Information with the Intelligence Community under the USA Patriot Act. *American Criminal Law Review, 39*(3), 1261+.
10. Connor, G.M. (2001) Banking aspects of the USA PATRIOT act: In a sense, banks have been deputized as federal law enforcement agencies. *New Jersey Law Journal, 166*(10), 24-25.
11. Current Hazmat Background Checks Hurt Trucking Says ATA. (2005, November 5). Capital Reports Environmental News Link. Retrieved July 20, 2007, from http://www.caprep.com/b1105003.htm
12. Dempsey, J. X. (2002) Civil liberties in a time of crisis. *Human Rights Magazine 29*(2) 23-34.

13. Etzioni, A. (2004). *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*. New York: Routledge.
14. General Accounting Office. (2004) *Aviation Security: Computer-Assisted Passenger Prescreening Challenges*. United States Department of Homeland Security, Transportation Security Administration.
15. Gerdes, Louise I. (2005) *The Patriot Act: Opposing Viewpoints.* Farmington Mills: Thomson Gale.
16. Gorman, M. (2006). Those Lost Liberties May Be Your Own. *American Libraries.* 37 (6), 5.
17. Henderson, N. C. (2002). The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications. *Duke Law Journal, 52*(1), 179+.
18. Herold, R. (2004, October). USA Patriot Act: Considerations for Business. Retrieved July 20, 2007, from www.informationalshield.com
19. Jaeger, P. T., Bertot, J. C., McClure, C. R. (2004). The USA PATRIOT act, the foreign intelligence surveillance act, and information policy research in libraries: Issues, impacts, and questions for librarians and researchers. *Library Quarterly, 74*(2), 99-121.
20. Jaschik, S. (2004) *Homeland security and the American Campus.* Priorities: Association of Governing Boards of Universities and Colleges.
21. Jonas, S., & Tactaquin, C. (2004). Latino Immigrant Rights in the Shadow of the National Security State: Responses to Domestic Preemptive Strikes. *Social Justice, 31*(1-2), 67+.
22. Kranich, N. (2006). The Impact of the USA Patriot Act: An Update. Free Expression Policy Project site. Retrieved July 17, 2007, from http://www.fepproject.org
23. Lee, L.T. (2003) The USA PATRIOT Act and telecommunications: Privacy under attack. *Rutgers Computer And Technology Law Journal 29*(4) 371-403.
24. Lilly, J. R. (2003). National security at what price? A look into civil liberty concerns in the information age under the USA PATRIOT act of 2001 and a proposed constitutional test for future legislation. *Cornell Journal of Law and Public Policy, 12*(2) 447-471, 443.
25. Martin, C. & Martin, S. (2005, May/June). The Impact of the USA Patriot Act on Records Management. [Electronic Version]. *Information Management Journal*.
26. Martyka, Jim. (2002) Critics: Patriot Act may be impossible to obey. *Minneapolis / St. Paul Business Journal*, 62(2), 7.
27. Oneill, R. (2006). Questioning Ohio's Loyalty Requirement. *Chronicle of Higher Education.* 53 (15), 24
28. Osher, Steven A. (2002) Privacy, Computers, and the Patriot Act: The Fourth Amendment Isn't Dead, but No One Will Insure It. *Florida Law Review*, 54, 521-542.
29. Paige, J. (2005, January 28). Patriot Act means more paperwork for bankers. [Electronic Version]. *Washington Business Journal*.
30. Patriot Act Chalks Up 310 Arrests; Justice Report Cites 'Al Qaeda's Worst Nightmare'. (2004, July 14). *The Washington Times*, p. A03.
31. Paye, J. (2006). A Permanent State of Emergency. *Monthly Review: An Independent Socialist Magazine.* 58(6). 29-37.
32. Pike, G.H. (2002) History repeated with the USA Patriot Act. *Information Today* 19(11) 19-21
33. Pike, G. H. (2007). The Patriot Act Illuminated. *Information Today.* 24 (5), 17-18.
34. Platt, T., & O'Leary, C. (2003). Patriot Acts. *Social Justice, 30*(1), 5+.
35. Plesser R.L. & Halpert JJ & Cividanes E.W. (2002) The USA Patriot Act for internet and communication companies. *The Computer and Internet Lawyer* 19(3) 1 – 9.
36. Podzolka, A., & Deberry, H. (2003). Patriot Act-Related Anti-Money-Laundering Requirements-The Hype and the Reality. *ABA Banking Journal*, 95(5), 63.
37. Pulley, M. (2004, August 6). Privacy, please. [Electronic Version]. *Sacramento Business Journal*.
38. Regan, P. M., (2004) Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly, 21*(4), 481-497.
39. Retired Air Force Sergeant Convicted of Espionage Try. (2003, February 21). *The Washington Times*, p. A03.
40. Rivard, N. (2002) USA PATRIOT act: How to be response ready: Concerned about protecting staff and student privacy while complying with new anti-terrorism laws? It's never too late to establish a chain of command, procedures, and protocols, say the experts. *University Business 5*(4), 43-48.

41. Romainiuk, P., Haber, J., & Murray, G. (2007). Suspicious Activity Reporting Regulatory Change and the Role of Accountants. *The CPA Journal.* 70-72
42. Sanders, Bernie. (2003) Unpatriotic Act. *Publisher's Weekly*, 250, 22.
43. Schriner, M. and Martinson J. (2003). It's a regulatory jungle out there! The USA PATRIOT Act, the RMA. *Rick Management Association Journal*, 85(7), 28-32.
44. Schwartz, E. (2006, April 17). The Compliance Headache. *Infoworld.* 28 (16). 12.
45. Sinnar, S. (2003). Patriotic or Unconstitutional? the Mandatory Detention of Aliens under the USA Patriot Act. *Stanford Law Review*, *55*(4), 1419+.
46. Strong Patriot Act Required. (2005, July 3). *The Washington Times*, p. B03.
47. Swanton, M. (2006, May). Boardroom Bugs. Retrieved July 17, 2007, from www.insidecounsel.com
48. Tiefer, C. (2004). *Veering Right: How the Bush Administration Subverts the Law for Conservative Causes*. Berkeley, CA: University of California Press
49. United States Department of Homeland Security. (2003). *US-VISIT Program, increment 1: Privacy impact assessment, executive summary.*
50. Wills, N. J. (2002). A Tripartite Threat to Medical Records Privacy: Technology, HIPAA'S Privacy Rule and the USA Patriot Act. *Journal of Law and Health*, *17*(2), 271+.
51. Wilson, J. (2002, February 15). Employers facing new post-Sept 11 issues. [Electronic Version]. *Dallas Business Journal.*
52. Woellert, L (2006). Boardrooms Crawling with Bugs. *Business Week*. 3983. 14.

NOTES