PATRIOT Act: Implications for Colleges and Universities

Edward T. Chapman and Donald G. Marks
Department of Computer Science, University of Tulsa, Tulsa, OK 74104

Quickly passed after the September 11 attacks, the PATRIOT Act has been supplemented with other acts in the past 3 yrs. Universities and schools must know the requirements and implications of these acts to ensure that their campus-wide information technology policies appropriately satisfy the requirements of the new anti-terrorism laws. Meeting these new security requirements demands information technology capabilities not normally implemented on university campuses. A university may need to implement a "pen register" to record all the routing information related to a specific student for up to 6 months. Care must be taken not to reveal more than the law allows. University computer policies and practice must be evaluated for conformity to current law. These new security and reporting requirements add to the Information Technology department's workload and mandate new capabilities for university IT departments. To address the new challenges, university IT departments must train or hire staff as well as allocate appropriate resources. *© 2005 Proceedings of the Oklahoma Academy of Science*

INTRODUCTION

The PATRIOT Act, passed after the September 11 attacks, was designed to provide law enforcement agencies with the necessary tools to combat terrorism and to generally improve their ability to combat crime. It defined new federal crimes for terrorist-related activities, money laundering, and fraudulent charities; raised penalties for existing crimes; and modified the procedures for tracking and gathering intelligence. Foreign intelligence investigation restrictions were loosened.

EFFECT ON COLLEGES AND UNIVERSITIES

Some of these changes to the law will affect colleges and universities, just as they will all large enterprises. Academic institutions, however, frequently have large numbers of foreign students on campus and therefore are tasked with enforcement of certain immigration laws. The PATRIOT Act mandated full compliance with existing immigration laws. In addition, the Internet is now a favorite mode of communication for students, a capability typically supplied by colleges and universities.

Three key acts were affected by the PATRIOT Act: Family Education Records Privacy Act (FERPA), Foreign Intelligence Surveillance Act (FISA), and Electronic Communications Privacy Act (ECPA) (Mitrano 2003). FERPA (20 United States Code 1232g) protects student records from unauthorized disclosures. The act was created during the Vietnam War to protect the privacy of students from real or perceived abuses by the federal government authority. The Foreign Intelligence Surveillance Act (50 U.S.C.) allows government agencies to avoid fourth amendment requirements if an activity is backed by a hostile foreign power. Seven special judges were appointed to oversee the execution of FISA provisions. Given the nature of FISA, the only information publicly available about its execution is the number of applications submitted for exemptions under FISA and the number of applications approved. The Electronic Communications Privacy Act (18 U.S.C.) describes the legal boundaries of government relating to computer networks. The ECPA is a technologically sensitive update for the Omnibus or "wiretapping" act. It outlines the privacy protections of electronic communications and any exceptions allowed.

The PATRIOT Act modified these acts in the following ways. The FERPA Act contains a clause that allows an institution to release a student's information to law enforcement if the safety and well-being of that student was threatened. Changes include a terrorism clause that permits the release of student information if it would protect the health and safety of others. There would be no liability in this case. No record of the action would be required.

FISA was modified to allow the government to obtain records related to an investigation of terrorism or spying. The organization would be indemnified from related disclosure penalties. The process remains secret, with the organization prohibited from disclosing any information about the orders. The number of special judges who could approve the requests was raised from 7 to 12. One key issue that must be satisfied is that the investigation not be solely based on protected First Amendment activities.

Civil rights groups have raised concerns about breaching the wall between foreign intelligence gathering and criminal investigation (Anonymous 2004). The concerns stem from lower standards for search and seizure. While abuse of power is always a possibility, not one case of abuse has been substantiated over the first 3 yrs of the act (Rozenwig 2004).

The PATRIOT Act modified EPCA in three ways. First, a business, institution, or operator may report imminent emergencies of a person's health or well-being. The report can be made to nearly anyone, not just the government. This modification is common sense and follows the lines of Good Samaritan laws already in effect in many states. The second modification allows operators to track unauthorized use of a system and to report the activity to law enforcement. This modification would be equivalent to being able to call the police if there was a robber in your house. Required disclosure to law enforcement through warrants and subpoenas is the third modification. The standard for issuing warrants or subpoenas are lowered, and judges are required to approve law enforcement requests that meet less than the accepted Fourth Amendment standard. The lower standard particularly applies to pen registers and trap and trace devices.

A pen register or trap and trace device records data about addressing, but not the content of a communication. For example, a pen register would record source, destination, and time as well as routing information. The purpose is to collect information about sites visited and times while not revealing the content or nature of what the person did. Neither of these need be actual devices. For modern networks, they are software programs that monitor network operation and save relevant data. On the other hand, law enforcement uses a wiretap to collect the content of the communication.

A subpoena requires an institution to provide technical assistance to collect and store this data for up 6 months. The PATRIOT Act provides reasonable compensation for expenses incurred while fulfilling the technical requirements. When a PATRIOT Act subpoena is used, the government request or the investigation results never need to be revealed to the people being monitored (Cox 2004).

The provider is absolved of liability for revealing information required by law. However, due diligence must be exercised by Information Technology departments not to reveal more than is required by law.

The PATRIOT Act does not change existing requirements. A previous law, Communication Assistance for Law Enforcement Act (CALEA, 1994) requires internet service providers (ISP) to limit law enforcement access to only material described in the court order. While the ISP is only required to provide technical assistance, CALEA specifies technical assistance as the telecommunication carrier implementing and maintaining the pen register, then providing the resulting data to law enforcement (Anonymous 2002).

The pen register, trap and trace device, or wiretaps all take the form of a Carnivore-like system digital collection system when implemented on a network (Orr 2002). Carnivore was originally developed for law enforcement and was championed before Congress in 2000 as a legitimate means to collect subpoenaed digital information on networks and from email. Eventually this system was replaced with a newer system with improved surveillance capabilities.

MULTI-DOMAIN UNIVERSITY NETWORK TOPOLOGIES

The fundamental issue, therefore, is that a law enforcement agency, such as the FBI, may subpoena a university IT department for records requiring the installation of a pen register as stipulated in PATRIOT Act section 216. Law enforcement expects the university to know how to do this; many universities expect the law enforcement agency to provide the necessary technical expertise. To ensure the integrity of pen register data, proper, thoughtful installation and maintenance is required. Improper installation may result in the disclosure of protected information, degradation of the university network, or even charges of failing to comply with the subpoena. A federal subpoena will typically require the university to collect all information about the target, from any computer under university control.

Many large universities and corporations have “multi-domain” networks. That is, the Law College may administer its own network, while the Engineering College administers a separate network. Users may have different user-ids on each domain, or they may have a single user-id for anywhere in the university. Multi-domain university or corporate networks present special challenges for pen register implementation. Perhaps most important is centralized authentication. Without centralized authentication, each domain must have some means of identifying users. Target lists and recorded information on each domain must be carefully maintained to ensure that the tracking does not exceed the limits of the judicial order. Such maintenance places more work on the shoulders of network administrative personnel. It also increases the chances of a serious error occurring that may render the collected evidence useless. Yet another issue would be ensuring that the expectation of privacy requirement is being protected for non-targeted users on university networks.

Some universities have open network policies that do not require any user login. This practice is disturbing on several levels. First, by letting a user either plug in a notebook computer or use an open computer in a library, there would be no way to differentiate between legitimate and malicious users until the network becomes threatened or damaged. Second, open systems make creating a pen register particularly onerous if not impossible. Without a reasonable method of determining whether or not a target is on a particular system, the only way law enforcement could know when a target is on the network is through visual surveillance and complete recording of all network communication for each and every machine across a network.

Even if a university has implemented centralized authentication and created standard system-wide policies, individual system administrators may not enforce all the policies consistently. Consequently, an attacker may only need to relocate on the network to carry out an attack. A domain administrator may circumvent the centralized authentication by creating domain level accounts that might allow the target to access the network without using the central authenticator.

Proper software patching and password integrity are other issues. If the authentication mechanism can be circumvented or defeated due to improper maintenance, the administrator and law enforcement cannot be reasonably certain that they have collected correct data. If users are allowed to share accounts, the resulting data will again be useless. Permitting weak passwords can also affect data integrity. If a target user can access another user's account, he or she becomes very difficult to track. Weak passwords can be prevented with readily available software packages. University policy must clearly and succinctly specify what must not be permitted. The university may even be held responsible for enforcing its IT policies. An effective user education program must be in place. Because of these obstacles, effective implementation of a pen register on a multi-domain network is particularly difficult.

IMPLEMENTING A DIGITAL COLLECTION SYSTEM—TECHNICAL ISSUES

Several issues must be considered for effective implementation of a pen register. University systems are typically set up as networks. However, they are rarely monolithic, instead they are comprised of many local area networks (LANs), each controlled by a particular department, college or campus. Authentication requests are submitted to a central server so that any authorized user may use any supported computer. This central authentication server will then need to notify the monitoring software on each segment of the network.

A commercial intrusion detection system (IDS) might be used to monitor each LAN. However, IDSs use hard-coded rules to track specific computers or IP addresses, not users. In addition, each LAN may have its own IDS, and there is no guarantee that they will all be compatible. Because the target user may move among the network segments, these IDS systems must coordinate activities to capture all the relevant data for the target.

The tracking system must be responsive enough to recognize whether the user is logged onto one or more computers and to track all sessions. It the user logs out, the system must end all recordings from that system to ensure that the privacy of other users are protected and that the integrity of the recorded data is not compromised. Subsequently, the monitoring system must be updatable on the fly.

If the target does not log off the system, data integrity cannot be guaranteed. If another user fails to log off, the target may hijack the session and the pen register will miss the data. Identifying hijacked sessions is impractical; however, setting the system up to force each machine into a locked hibernation state or forcing users off after periods of extended inactivity could minimize this problem and make for a more secure network.

If the target moves to a different logical domain, the system must be able to respond to the change by initiating a new rule on the separate domain. If authentication is domain based, the problems become more complex because the pen register would need to be controlled from each domain. This may allow domains sharing physical network resources to monitor the activities of other domains. Such action would create a host of legal, ethical, and psychological acceptability issues. As long as centralized authentication remains in place, this should not be an issue. However, this does mean that the pen register must also be implemented outside of the confines of a lower organizational unit or domain.

Open networks are open to any person who has physical access to the machine. Because pen registers must associate data with a particular person, it is not clear how to implement a pen register, or even if pen registers are of any value in open systems.

HOW COLLEGES AND UNIVERSITIES SHOULD RESPOND

The university may handle the pen register or trap and trace subpoena in one of three ways. First, the university may open up its networks to law enforcement and allow them to install any equipment they see fit while trusting them to only gather information in strict accordance with the subpoena. Second, the university may assign personnel to work closely with law enforcement to ensure that the equipment installed and the information gathered does not exceed the boundaries of the court order. Third, the university may use an internal implementation of a proven system to collect and deliver subpoenaed data to law enforcement.

No option is without risk. For the first option, the university trusts that the law enforcement agency will not exceed the bounds of the warrant. Sometimes an officer exceeds the bounds of the warrant. In a 1991 case, Steve Jackson Games sued the Secret Service for violations of both the Privacy Protection Act (PPA) and ECPA after the Secret Service confiscated a computer that contained 162 private, unopened emails not within the limits of the warrant. The court awarded SJG in excess of $300,000 in the judgment. There still are legal risks for civil lawsuits for the university. One 1998 case held a service provider civilly liable for ECPA violations when they revealed protected information to a law enforcement official (Clifford 2001). The reputation of the university must be considered. Damaging information could be illegally released in the course of the investigation. The result could be a public relations nightmare as well as a very expensive legally. Finally, the university assumes that law enforcement will have the necessary technical ability.

A subpoena for network tracking implies the implementation of a Carnivore-like system on the university network. There may be one or multiple implementations on the network. Such implementations could wreak havoc on the network infrastructure without thoughtful interaction with university IT personnel. The university blithely trusts that only subpoenaed data will be collected. Furthermore, if law enforcement lack the necessary skills to collect what they need on site, they will confiscate systems for analysis at another location. In 1998, a district court ruled in the U.S. vs. Hunter case that law enforcement must confiscate equipment if they do not have technical or practical means to search computers on site (Clifford 2001). While the university is obligated to fully comply with the requirements of the subpoena, the immediate and complete removal of an email server may be difficult for a university network administrator to smoothly manage any network.

The second option avoids some pitfalls by assigning personnel to handle the subpoena. The people assigned must include university counsel and a very knowledgeable IT manager. The approach should be to build a working relationship with the law enforcement personnel. The counsel will check the court order to determine what the law enforcement needs to collect and that they have completed the order appropriately. The purpose is to protect the university. Make certain of what is required and make certain of what is delivered. The IT manager will then take a list of what is required from the university counsel and help law enforcement collect what they need. The advantage to this approach is that the counsel and IT manager will know what cannot be taken as well as what can be. More importantly, if law enforcement must implement a digital collection system on a network, it can be done strategically. This will allow minimal impact on the network while also protecting the university's interests. This option would work with some planning and judicious network policy implementations.

Finally, the university might assume responsibility for collecting and delivering required information to law enforcement as prescribed in the PATRIOT Act. This would require investing a system that meets the requirements for court admissible evidence. Care must be taken as improper collection may result in very large civil lawsuits. In a 2002 case, George Mason University constructed an internal digital collection system to catch a hacker. The hacker was caught and arrested on the collected evidence. When the case went to court, the evidence was thrown out because their internal system did not meet the court admissible evidence requirements. George Mason University's case subsequently collapsed and the accused hacker was released. The accused hacker countersued the university and won a multimillion dollar lawsuit (Ryan 2005).

Two advantages of an internally implemented system would be that the system could be used to track and prosecute hackers and that law enforcement would not need to implement a Carnivore-like system on the university network. In this case, law enforcement would present the subpoena to university counsel, who would in turn direct the IT department to implement rules to collect required information. The information, along with supporting documentation, would be turned over to law enforcement as prescribed by the court order. This would allow the university near complete control of information released and allow the university minimal legal exposure while protecting the privacy of the university family.

In all three cases, USA PATRIOT Act section 225 provides immunity for release of information in "accordance with a court order." As exemplified by the three cases mentioned above, therefore, it is imperative that the university does not deviate from the specifics of the court order to avoid litigation. (Tribbensee 2004)

CONCLUSIONS

The IT department needs to make any necessary changes to their operational procedure before being contacted by law enforcement so that the plan can be executed easily and efficiently. The department will need to install appropriate hardware and software that will aid in protecting university networks. The IT department and legal department must develop a specific policy that designates responsibility and outlines procedures. The policy should address the following issues:

- Warrants, subpoenas, and incidental contact with law enforcement.
- Illegal and unauthorized activity taking place on university networks—identify and stop it.
- Emergency disclosures.

Consulting with legal counsel will be needed to protect the university. There may be legal issues if the IT department is unable to obtain the data specified in the legal order. However, supplying too much information by allowing law enforcement full access to all the data may create more legal issues. Polices and procedures will need to be evaluated for compliance. In addition, requests from law enforcement must be reviewed for correctness. Any information released must not exceed the limits of the law.

The provisions for the pen registers, trap and trace devices, and wiretaps do not have a sunset and will continue to be law after other parts of the PATRIOT Act expire.

Colleges must maintain the delicate balance between cooperation and disclosure when handed a court order for digital information. While a university must comply with the particulars of a court order, they must also be mindful of the need to protect the privacy of the university family and keep the institution safe from civil lawsuits.

REFERENCES

[Anonymous]. 2002. Summary of CALEA requirements. TIA TR45 Lawfully Authorized Electronic Surveillance Ad Hoc, Version 2.1, November 16. p 11.

[Anonymous] 2004. The USA Patriot Act [online]. Electronic Privacy Information Center. Available from: http://www.epic.org (Accessed 8/20/2004).

Clifford R. 2001. CyberCrime-the investigation prosecution and defense of computer related crime. Durham(NC): Academic Press. 194 p.

Cox J. 2004. IT departments must cope with the Patriot Act, university CIO says [online]. Network World Fusion, August 3. Available from: http://www.networkworld.com/news/2004/0803patriot.html (Accessed 3/20/2005)

Mitrano T. 2003 Civil privacy and national security legislation: A three dimensional view. Educause Rev 38(6):52-62.

Orr A. 2002. Marking Carnivore's territory: rethinking pen registers on the internet [online]. 8 Mich Telecomm Tech L Rev 219. Available from: http://www.ttlr.org/voleight/orr.pdf (Accessed 4/16/2005)

Rozenzwieg P. 2004. Face facts: Patriot Act aids security, not abuse. Christian Sci Monitor 96(171):9.

Ryan D. Shpantzer G. 2005. Legal aspects of digital forensics, George Washington University [online]. Available from: http://www.danjryan.com/Legal Issues.doc (Accessed 4/16/2005).

Tribbensee N. 2004. Privacy and security in higher education computing environments after the USA PATRIOT Act. J Coll Univ Law 30(2):348.

USA PATRIOT ACT of 2001. Pub L 107-56, 15 Stat 272 (Oct. 26, 2001).

Received: April 14, 2005; Accepted December 6, 2005