NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 5
Issue 2 *Spring 2004*

Article 1

3-1-2004

The USE Patriot Act: A New Way of Thinking, an Old Way of Reacting, Higher Education Responds

David Lombard Harrison

The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting, Higher Education Responds

David Lombard Harrison[1]

I. Introduction

On October 26, 2001, only six weeks after the unfathomable horror of September 11, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("PATRIOT Act").[2] The bill was more than 340 pages long, had significant changes in its final days, and affects more than fifteen already existing statutes.[3] In response to the crisis of September 11, the legislation passed 98 to 1 in the Senate and 357 to 66 in the House of Representatives without hearings and with little debate or discussion. Yet, the debate is increasingly being heard above the

[1] Associate Vice President for Legal Affairs, Office of the President, The University of North Carolina.

[2] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 18 U.S.C., 50 U.S.C., 22 U.S.C., 31 U.S.C., and 47 U.S.C.). The Act contains ten titles and addresses myriad issues, including: terrorism investigation funding, immigration requirements, the enhancement of federal authorities, assistance for terrorism victims, sharing of information among law enforcement agencies, bioterrorism prevention, and enhanced surveillance activities. *Id.*

[3] The statutes include the Federal Wiretap Statute, 18 U.S.C. §§ 2510–20 (2000) (Title III); the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801–29 (2000); Exec. Order No. 12,333 (1982); the Cable Act, 47 U.S.C. § 551 (2000); the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Federal Rules of Criminal Procedure (FED. R. CRIM. P.); and the Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 49-495, 100 Stat. 1243 (18 U.S.C. §§ 111, 202), which contains the Stored Wire and Electronic Communications Act, 18 U.S.C. §§ 2701–11; and the Pen Register and Trap and Trace Statute, 18 U.S.C. §§ 3121–27.

din of crisis, with members of the higher education community deeply involved;[4] even members of Congress have questioned their own actions voting for the Act.[5] Essential to this growing debate is the frank realization that the PATRIOT Act was implemented in response to a national security crisis, rather than an unfolding legislative action. Similar responses to actual or perceived security crises resulted in The Alien and Sedition Acts of 1798, President Lincoln's suspension of habeas corpus during the Civil War, the Espionage Act of 1917, the internment of Japanese-Americans after Pearl Harbor, and the Smith and McCarren Acts, during the McCarthy years.[6] Historical perspective, however, reveals these to

---

[4] The 2003 North Carolina Journal of Law & Technology Symposium, *The PATRIOT Act, Consumer Privacy, and Cybercrime*, exemplifies the role higher education has in leading the intellectual examination of the PATRIOT Act. While librarians have been most vocal about potential abuses of the PATRIOT Act, other members of higher education have also fully engaged in the dialogue on both sides. *See, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2002).

> This Article argues that the common wisdom on the USA Patriot Act is incorrect. The Patriot Act did not expand law enforcement powers dramatically, as its critics have alleged. In fact, the Patriot Act made mostly minor amendments to the electronic surveillance laws. Many of the amendments merely codified preexisting law. Some of the changes expanded law enforcement powers, but others protected privacy and civil liberties. . . . The Patriot Act is hardly perfect, but it is not the Big Brother law many have portrayed it to be.

Id. at 608.

[5] Representative C.L. "Butch" Otter, a Republican member of Congress from Idaho, offered an amendment to the Commerce, Justice and State funding bill that prohibits federal law enforcement agencies from implementing "sneak and peek" search warrants. The bill passed by a vote of 309 to 118, with 113 Republicans voting in favor of it. In response to the growing criticism, Attorney General John Ashcroft took his defense of the Act on the road. PBS, *Online NewsHour: Weighing the Patriot Act: Background* (Aug. 19, 2003), *at* http://www.pbs.org/newshour/bb/terrorism/july-dec03/patriot_8-19.html (on file with the North Carolina Journal of Law & Technology).

[6] *See* William J. Brennan, Jr., *The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crises*, Address Before the Law School of Hebrew University, Jerusalem, Israel (Dec. 22, 1987), *at* http://www.brennancenter.org/resources/downloads/nation_security_brennan.pdf (on file with the North Carolina Journal of Law & Technology); *see also* Johnathan R. Cole, *The*

have been reactions, rather than responses, and none of these reactions is defensible today; most must be viewed as reprehensible and unjustified reactions to perceptions of the need for expediency in the face of perceived threats to national security.

The core of the debate is one central to the fundamental American struggle: freedom versus security and individual will versus the public good.[7] The tensions that are inherent in the debate between surveillance needs and the preservation of civil liberties have their roots in the fundamental struggle of community interests versus individual interests—a struggle that has defined much of the history of the United States, from the Declaration of Independence through the Constitution, Bill of Rights, and the statutes and judicial interpretations that have followed. Because of the nature of the American tension between individual and community interests, the provisions of the PATRIOT Act are certain to be challenged, modified, and supported by more acts of Congress, interpretations by the judiciary, and orders from the executive branch. In fact, the Bush Administration and Congress have already strengthened the surveillance powers of the PATRIOT Act.[8]

It is certainly naive to reject surveillance as a necessary national tool,[9] and critics blamed the naivety in rules for

---

Patriot Act on Campus: Defending the University Post-9/11, 28 BOSTON REVIEW 3T (2003).

[7] *See, e.g.*, SARAH VOWELL, PARTLY CLOUDY PATRIOT 33 (2003).

[8] Intelligence Authorization Act for Fiscal Year 2004 gives law enforcement access to financial institution records by use of a "national security letter," rather than a subpoena. *See* Kim Zetter, *Bush Grabs New Power for FBI*, WIRED NEWS (Jan. 6, 2004), *at* http://www.wired.com/news/print/0,1294,61792,00.html (on file with the North Carolina Journal of Law & Technology) (citing Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, 117 Stat. 2599 (codified as amended in scattered sections of 31 U.S.C., 50 U.S.C., 5 U.S.C., 21 U.S.C., 42 U.S.C., 18 U.S.C., and 8 U.S.C.)).

[9] The surveillance and privacy debate is not new. Henry Stimson, known for making one of the most memorable statements concerning the ethics of surveillance, said,

> After he entered the White House in 1933 . . . [Franklin D. Roosevelt] quickly resumed his interest in intelligence. Four years before, Henry Stimson, the Secretary of State, had abolished the "Black Chamber," the nation's first peacetime

intelligence gathering as a reason for the devastating success of the September 11 operation.[10] However, the toll on civil liberties in times of war and crisis has been high. As United States Supreme Court Justice William J. Brennan, Jr. acknowledged:

> When I think of the progress we have made over the last thirty years, I look upon our system of civil liberties with some satisfaction, and a certain pride. There is considerably less to be proud about, and a good deal to be embarrassed about, when one reflects on the shabby treatment civil liberties have received in the United States during times of war and perceived threats to its national

---

> codebreaking agency, famously declaring, "gentlemen do not read each other's mail." Later, in the shadow of Pearl Harbor, critics would claim that this had neutered American codebreaking during the 1930's. In reality, it merely redirected it into more secret channels in order to conceal it from an isolationist nation and Congress. The army set up its Signals Intelligence Service under the codebreaking genius, William Friedman, and by the mid-1930's it was regularly cracking Japanese diplomatic ciphers. By the end of the decade these were being discreetly circulated in Washington under the codename "Magic."

DAVID STAFFORD, ROOSEVELT AND CHURCHILL, MEN OF SECRETS 7 (1999). It is interesting that the FBI has recently developed its own "Magic Lantern," which is a computer Trojan horse surreptitiously delivered by e-mail, and capable of recording every keystroke of a computer. Magic Lantern, which the FBI admitted in December of 2001 is "under development," is not new technology—it has been a hacking device for several years. *See* Robyn Weisman, *FBI Waves 'Magic Lantern'*, News Factor Network (Dec. 31, 2001), *at* http://www.newsfactor.com/perl/story/15301.htm (on file with the North Carolina Journal of Law & Technology). It is a Trojan horse (similar to a "virus") sent through e-mail, which captures every keystroke typed by a person, after it installs itself on the target computer. By capturing the keystrokes, passwords can be obtained and then encrypted documents can be opened with the password. In addition, keystrokes can recreate all activities of the computer user. While Magic Lantern's delivery is novel for law enforcement, key logging is not. The FBI has installed key loggers in criminal investigations (pursuant to a "sneak-and-peek" search). *See, e.g.*, United States v. Scarfo, 850 F.2d 1015 (D.N.J. 2001).

[10] *See, e.g.*, Stewart Baker, *Wall Nuts: The Wall Between Intelligence And Law Enforcement Is Killing Us*, SLATE (Dec. 31, 2003), *at* http://slate.msn.com/id/2093344 (on file with the North Carolina Journal of Law & Technology).

> security. For as adamant as my country has been about civil liberties during peacetime, it has a long history of failing to preserve civil liberties when it perceived its national security threatened. This series of failures is particularly frustrating in that it appears to result not from informed and rational decisions that protecting civil liberties would expose the United States to unacceptable security risks, but rather from the episodic nature of our security crises. . . .
>
> The sudden national fervor causes people to exaggerate the security risks posed by allowing individuals to exercise their civil liberties and to become willing "temporarily" to sacrifice liberties as part of the war effort.[11]

It is this historical context and philosophical uneasiness that must add fuel to the emerging debate surrounding the PATRIOT Act.

Title II of the PATRIOT Act was meant to be a solution to one of the first questions everyone asked on September 11: How could this have happened without the FBI and CIA knowing about it?[12] However, Title II's solution, which broadens the powers of law enforcement and national security agencies to conduct surveillance, has had a significant impact on the use of surveillance technologies and will arguably affect the privacy interests of everyone, not just the "terrorists" who are the intended targets. The message from the Department of Justice is that there is a need for more tools in the fight against terrorism: "The Patriot Act gives us the technological tools to anticipate, adapt, and outthink our terrorist enemy. To abandon these tools would senselessly imperil American lives and American liberty, and it would ignore the lessons of September 11."[13] But are we being asked to give up

---

[11] Brennan, *supra* note 6.

[12] The focus of this article is primarily on Title II, which concerns surveillance and privacy issues, and other Titles that particularly affect higher education.

[13] PBS, *supra* note 5; *see also* Jerry Seper, *Ashcroft says USA Patriot Act needed to stop terrorists*, WASH. TIMES (Aug. 20, 2003), at A03, *available at* http://washingtontimes.com/national/20030819-110617-8552r.htm (on file with the North Carolina Journal of Law & Technology).

essential liberty in the name of a little temporary security?[14]

Title II of the PATRIOT Act has received the most attention because of the provisions concerning "roving wiretaps," "sneak-and-peek" warrants, Carnivore applications, lowered standards for gaining surveillance authority, and other technical issues. However, it's less obvious result is a fundamental removal of the walls that once existed between the FBI and national security agencies, and a removal of the internal wall in the FBI that segregated intelligence gathering from criminal investigation.[15]

> "We are going to have to get used to a new way of thinking," Assistant Attorney General Michael Chertoff, who is in charge of [investigating] the Sept. 11 attacks, said in an interview. "What we are going to have is a Federal Bureau of Investigation that combines intelligence with effective law enforcement."[16]

---

[14] "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." Benjamin Franklin, Pennsylvania Assembly: Reply to the Governor (Nov. 11, 1755), *in* 6 THE PAPERS OF BENJAMIN FRANKLIN 242 (Leonard W. Labaree ed.) (1963). This is especially a concern if tools in the PATRIOT Act may reflect more a "wish list" for ordinary criminal investigation, rather than specific and targeted anti-terrorism techniques. *See* Peter Erlinder, *Revelations of Pre-September 11 Warnings Require PATRIOT ACT Repeal,* MINNEAPOLIS STAR TRIBUNE, May 22, 2002, at

[15] *See* Federal Bureau of Investigation, *Federal Bureau of Investigation War on Terrorism Counterterrorism, Intelligence and Analysis*, *at* http://www.fbi.gov/terrorinfo/counterrorism/analysis.htm (on file with the North Carolina Journal of Law & Technology).

> The PATRIOT Act and a federal court decision in November 2002 have broken down what has been known as "the Wall" that legally separated law enforcement and intelligence functions. As a result, coordination and information sharing between the law enforcement community and intelligence agencies have been greatly improved. Since the attacks of September 11, the cultural and operational wall between the FBI and CIA has also been broken down, with the two agencies becoming integrated at virtually every level of operation.

Id.

[16] Jim McGee, *An Intelligence Giant in the Making*, WASH. POST, Nov. 4, 2001,

This new way of thinking is the abandonment of post-Watergate policy decisions to separate intelligence and law enforcements functions to prevent abuses by the FBI and national security agencies.[17] To many, this is the real concern with the PATRIOT Act. Roving wiretaps, sneak-and-peek searches, and the host of "tools" allowed by the Act are already in limited use, but the rearrangement of law enforcement and national security agencies is a return to an old way.

Colleges and universities must also get used to a new way of thinking because they have an unmatched intersection of high technology and foreign nationals—the explicit primary concerns of the PATRIOT Act. Moreover, institutions of higher learning are microcosms of the struggle between individual rights and the public good, and are, by nature, forums for the most difficult debates, with members of the higher education community often at the forefront of the issues. The question is whether higher education will be part of the response or part of the reaction.

This article first recognizes the tension between individual

---

at A04.

[17] *See* RICHARD A. BEST, JR., INTELLIGENCE AND LAW ENFORCEMENT: COUNTERING TRANSNATIONAL THREATS TO THE U.S. 13 (footnote omitted) (2001).

> In some cases, efforts of intelligence agencies in support of law enforcement efforts proved to be ill-advised. In particular, instances of intelligence agencies acquiring information concerning U.S. citizens or persons has been widely condemned. In addition to various questionable Cold War activities, such as mail openings and involvement with the Mafia, the CIA and military intelligence units gathered intelligence on antiwar groups within the United States during the Vietnam War period.
>
> Such activities served as a major impetus for wide-ranging congressional investigations of the U.S. Intelligence Community in the 94th Congress.
>
> In the aftermath of sensational revelations about improper activities by intelligence agencies, both the Intelligence Community and its congressional overseers were determined to separate the work of intelligence and law enforcement agencies in order to prevent the use of intelligence techniques against citizens and legal residents of the United States unless court orders have been obtained.

freedom versus the community good in surveillance activities, the unjustified reactions taken in times of security crises, and Title II of the PATRIOT Act's creation of a new way of thinking after September 11. The article then examines the means and methods of surveillance, and the significant changes made to existing surveillance laws by Title II. The article also examines how section 215 of Title II generated a debate between librarians and the Justice Department that revealed the need for and importance of that debate in determining whether the PATRIOT Act is a reaction or a response to a perceived security crisis. The article then examines provisions outside Title II, which have a significant effect on institutions of higher education. The article concludes by accepting higher education's duty to advance the debate between individual freedom and the community good, and also higher education's need to respond with practical solutions.

II. Methods of Surveillance and Information Gathering

For many concerned with the PATRIOT Act, the starting point is the Fourth Amendment,[18] and its first mandate that the government cannot intrude when one has a reasonable expectation of privacy; and its second mandate that permitted intrusions are to be regulated and open.[19] In response to the September 11 attacks,

---

[18] U.S. CONST. amend. IV.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

[19] Although the PATRIOT Act concerns surveillance by the government, it must also be understood that in this digital information age, expectations of privacy on the Internet are, for the most part, unreasonable. While Sun Microsystems CEO Scott McNealy's statement "You have zero privacy, anyway. Get over it," may be extreme, no institution of higher education acting as an Internet service provider or other provider of communications can guarantee absolute privacy. Any expectation of privacy on the Internet or local area network should be replaced with a frank realization that privacy cannot be promised to any user of Internet or network computer resources, because the technology leaves a clear

the PATRIOT Act thrusts the Fourth Amendment back to the forefront of the national consciousness. Title II fundamentally changes the relationship of a communications provider to those it serves and increases the power of law enforcement to perform surveillance and to retrieve information.[20] These changes are seen by many, on all sides of the political and civil liberties spectrum, as significantly altering the privacy landscape in the United States of America.[21]

---

and lasting trail of a user's activity. Internet use, network use, and e-mail are, by their very nature, not private and there should never be any expectation of privacy in their use. Information is shared, copied, stored, and disseminated repeatedly and indiscriminately, all as a matter of transmission and delivery. The overall lack of privacy does not, however, mean that any user of institution resources should be subject to unreasonable interference from other users or unreasonable access from either the institution or government entities. Thus, IT policies should address the limitations of access and interference, and disclosure protocols should protect unreasonable access and interference. In addition, users should be aware that the institution adheres to all applicable laws that protect the members of the institution community—including the PATRIOT Act.

[20] For example, Title II of the Act:

- Allows an Internet Service Provider (ISP) to voluntarily disclose content and other information from its users in situations it deems to be an emergency;
- Permits intelligence and law enforcement to share previously protected information;
- Increases the power of law enforcement to track suspects with "roving wiretaps," which may be placed on any phone or other communications device;
- Allows voice-mails to be seized with a warrant, rather than a wiretap order;
- Enhances the ability and power to track suspects on the Internet;
- Allows an ISP to enlist the assistance of law enforcement to track and resist hackers or other computer "trespassers";
- Broadens secret "sneak-and-peek" searches where law enforcement can enter premises without notice;
- Lowers evidentiary standards for seeking information, making surveillance and information retrieval easier; and
- Opens the door to allowing law enforcement to secretly install software on individual computers or deliver surveillance software by Trojan horse e-mails.

[21] There are additional First Amendment concerns as well, such as whether the PATRIOT Act will have a chilling effect on free speech and assembly.

A. Types of Communication

The methods of surveillance and information gathering have paralleled the advance of technology, but the laws have not. Many of the changes enacted by Title II of the PATRIOT Act are a reply to those advances in technology and infrastructure, and the inconsistencies in the ways different technologies were treated. The methods themselves range from decades-old telephone wire technology to, as yet, unconfirmed worldwide systems which sweep and sort every byte of data from every source.[22] The surveillance laws specify three basic types of communication that can be gathered: oral, wire, and electronic communications. Oral communication is a human utterance made when the speaker reasonably expects that the utterance will not be intercepted. It does not include an electronic communication.[23] Wire communication is a human utterance transmitted in whole or in part over wire, cable, or similar connection furnished by a telecommunications facility; it did not include the portion of a communication transmitted by a cordless telephone until 1994.[24] Electronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.[25]

B. Methods of Surveillance

There are three general methods of information gathering that are at issue with Title II of the PATRIOT Act: wiretaps, pen/trap devices, and Internet/computer gathering devices. A wiretap is a device that intercepts the content of an oral, wire, or electronic communication through the use of any mechanical, electronic, or other device.[26] "Content" means any information

---

[22] *See, e.g.*, Echelon Watch, http://www.echelonwatch.org/ (last visited Mar. 16, 2004) (on file with the North Carolina Journal of Law & Technology).
[23] 18 U.S.C. § 2510(2) (2000).
[24] *Id.* § 2510(1).
[25] *Id.* § 2510(12).
[26] *Id.* § 2510(4).

concerning the substance, purport, or meaning of that communication.[27] A pen register is a device that is attached to a telephone line and which records all telephone numbers dialed out from a phone on that line.[28] A trap and trace device is a device attached to a telephone line, which records the number of each telephone dialing into that line.[29] They are treated identically in federal surveillance laws.

The newest methods are those that gather information from the Internet, and include Carnivore and DragonWare "taps." The FBI describes Carnivore, now known by the less-threatening name of DCS-1000, as a "surgical" ability to intercept and collect the Internet communications that are the subject of the lawful order, while ignoring those communications they are not authorized to intercept.[30] Those who have analyzed the system state that DCS-1000 is part of a suite of tools (known as DragonWare) including Packeteer and Coolminer, which can combine to recreate Web pages exactly as a surveillance subject saw them.[31] DCS-1000, alone, is a Windows-based system built with both commercial and proprietary software, which "sniffs" packets of information traveling on the Internet and then copies them. Because all information on the Internet travels in packets, some have challenged the "surgical" ability of DCS-1000.[32] Magic Lantern and Key Loggers are also new technologies to gather information

---

[27] *Id.* § 2510(8).
[28] *Id.* § 3127(3).
[29] *Id.* § 3127(4).
[30] *Internet and Data Interception Capabilities Developed by FBI, Hearing Regarding the Carnivore System Before the House Comm. on the Judiciary, Subcomm. on the Constitution*, 106th Cong. 67–305 (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation), *at* http://www.fbi.gov/congress/congress00/kerr072400.htm (on file with the North Carolina Journal of Law & Technology).
[31] Kevin Poulsen, *Carnivore Details Emerge* (Oct. 4, 2000), *at* http://www.securityfocus.com/ news/97 (on file with the North Carolina Journal of Law & Technology).
[32] *See* Catherine M. Barrett, *FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy*, 8 RICH. J.L. & TECH. 16 (2002), *at* http://www.law.richmond.edu/jolt/v8i3/ article16.html (on file with the North Carolina Journal of Law & Technology).

from the Internet. Magic Lantern, which the FBI admitted in December of 2001, is "under development," is not new technology—it has been a hacking device for several years.[33] It is a Trojan horse (similar to a "virus") sent through e-mail that captures every keystroke typed by a person, after it installs itself on the target computer. By capturing the keystrokes, passwords can be obtained and then encrypted documents can be opened with the password. In addition, keystrokes can recreate all activities of the computer user. While Magic Lantern's delivery is novel for law enforcement, key logging is not. The FBI has installed key loggers in criminal investigations, pursuant to a "sneak-and-peek" search.[34]

C. Procedures for Requesting Access

The surveillance laws allow many different agencies to collect information. The agencies include all of the Department of Justice agencies (e.g., FBI), other federal law enforcement agencies (e.g., Postal Inspectors, ATF), National Security agencies (e.g., CIA), and state agencies. In addition, all states have their own wiretapping and surveillance laws, as well as privacy laws. The Computer Crime and Intellectual Property Section of the Department of Justice ("CCIPS") has issued a comprehensive manual on searching and seizing computers and obtaining electronic information.[35] The CCIPS Appendix section contains examples of typical orders, warrants, and requests.

Generally, there is a "hierarchy" of complexity in requesting information, with the complexity increasing as the information becomes more protected. The lowest is the simple request, without any formal document, for information that is public or readily available without an expectation of privacy, or is

---

[33] Robyn Weisman, *FBI Waves 'Magic Lantern'* (Dec. 13, 2001), News Factor Network, *at* http://crmdaily.com/story.xhtml?story_id=15301 (on file with the North Carolina Journal of Law & Technology).

[34] United States v. Scarfo, 850 F.2d 1015 (D.N.J. 2001).

[35] DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *at* http://www.usdoj.gov/criminal/cybercrime/l&smanual2002.html (on file with the North Carolina Journal of Law & Technology).

being provided with consent. A letter request is the next level. It will specify the information being sought.[36] A subpoena is the next level and, although it is a court document, a federal official, rather than a court issues it.[37] A search warrant is more difficult than a subpoena and must be issued from a court on the basis of probable cause. It will be specific in its requirements and items sought.[38] A pen/trap order is more difficult to obtain and contains very specific information.[39] A pen/trap order can be issued by either a federal judge or a federal magistrate judge and must state: (1) the person in whose name the telephone line to which the device will be attached is listed, (2) the identity of the target of the investigation, (3) the telephone number and physical location of the telephone line to which the device will be attached, and (4) a statement of the offense to which the telephone numbers likely to be obtained relate.[40] There is no provision to notify those whose communications have been intercepted by a pen/trap. A pen/trap order may be issued for any crime.[41] A wiretap order is the most difficult to obtain.[42] A wiretap order, which can be issued only by a federal judge, must specify the following: (1) the identity of the target, (2) the location of the wiretap, (3) the type of communications to be intercepted and the particular offense to which the communications relates, (4) the identity of the agency authorized to intercept the communications and of the attorney authorizing the application, and (5) the period of time during which interception is permitted and whether the interception must terminate when the communications sought are first obtained.[43] The order also must state that the interception (1) shall be executed

[36] *See, e.g., id.* at app. C.
[37] *See, e.g., id.* at app. E.
[38] *See, e.g., id.* at app. F.
[39] *See, e.g., id.* at app. D.
[40] 18 U.S.C. § 3123(b) (2000).
[41] *Id.* § 3122(2).
[42] There are unique circumstances where a law enforcement officer, designated by a high-ranking Justice official, may authorize a wiretap without an order. In addition, there are many exceptions to the notice and the procedural provisions from consent to exigent circumstances and an order is not always required to collect information.
[43] 18 U.S.C. § 2518(4).

as soon as practicable, (2) shall be conducted in such a way as to minimize the interception of communications not within the scope of the order, and (3) must terminate upon attainment of the objective of the interception or in thirty days, whichever is sooner.[44]

III. Significant Changes to Existing Surveillance Laws

A. The Federal Wiretap Statute

The Federal Wiretap Act was enacted in 1968 and is often referred to as "Title III."[45] It generally requires a "probable cause" wiretap order from a judge to intercept real-time contents of voice and data communications. An affidavit from the government must support the request for the order. A wiretap will only be allowed for certain serious predicate crimes listed in the Act, and there is a duty to minimize the interception of information that is not relevant to the investigation. A wiretap order is more difficult to obtain than a search warrant because interception of communication has been held to be the most serious intrusion into the right of privacy. A wiretap order for oral or wire communications may be issued only for specific serious felonies.[46] A wiretap order to intercept electronic communications may be issued for any federal felony.[47] Targets who have had their communications intercepted must be notified of the interception no later than ninety days after completion of the wiretaps.

Prior to the PATRIOT Act, the wiretap statute allowed an ISP to monitor activity on its system to protect its rights and property, but it was not clear under prior law that the ISP could enlist the assistance of law enforcement when it discovered a hacker ("computer trespasser"). Section 217[48] of the PATRIOT Act allows, but does not require, an ISP to enlist the assistance of law enforcement and protects the government from liability if it

---

[44] *Id.* § 2518(5).
[45] *Id.* §§ 2510–20.
[46] *Id.* § 2516(1)(a)–(p).
[47] *Id.* § 2516(3).
[48] Entitled "Interception of Computer Trespasser Communication."

conducts warrantless wiretaps of computer trespassers. The trespasser's activity need not relate only to terrorism. A "computer trespasser" does not include a person "known by the owner or operator . . . to have an existing contractual relationship with the owner or operator."[49] Thus, an ISP cannot use this statute against one of its own users. Unfortunately, the section does not extend explicit immunity to the ISP for authorizing or enlisting law enforcement surveillance.

Section 202[50] also amends Title III[51] and allows a wiretap order to intercept wire communications (involving the human voice) for violations of the Computer Fraud and Abuse Act.[52] This amendment allows investigators to intercept online human voice transmissions when investigating hacking offenses.

B. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 ("ECPA")[53] regulates access to stored e-mail, other electronic communications, and transactional records of subscribers and users of a service. A warrant, issued on probable cause, is required for newer e-mail, but transactional records may be obtained by use of an administrative subpoena, which is much easier to obtain than a warrant. Section 209[54] reverses federal case law[55] and the ECPA,[56] which required law enforcement to seize voicemail messages with a wiretap order rather than a search warrant. This amendment makes access to voicemail the same as for e-mail. Section 210[57]

---

[49] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 217.

[50] Entitled "Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuse Offenses."

[51] 18 U.S.C. § 2516(1) (2000).

[52] *Id.* § 1030.

[53] The Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 49-495, 100 Stat. 1243.

[54] Entitled "Seizure of Voice-mail Messages Pursuant to Warrants."

[55] United States v. Smith, 155 F.3d 1051 (9th Cir. 1998).

[56] 18 U.S.C. § 2510(1) (2000).

[57] Entitled "Scope of Subpoenas for Records of Electronic Communications."

amends 18 U.S.C. § 2703 to allow investigators to use a subpoena for a broader array of Internet service subscriber information. This information now includes "the means or sources of payment for such services," "records of session times and durations," and "any temporarily assigned network address."[58] These provisions are meant to make the ECPA technologically current and also to provide the means to ascertain identities of individuals who use anonymous or erroneous biographical data on Internet accounts. The financial information is limited, however, to the bank account number or credit card information used as a means to pay for the communication service. A subpoena can also be used to gain e-mails if they are older than six months and the government has followed the required procedures.

Of considerable note is the new ability for law enforcement to have nationwide service for search warrants. Section 220[59] amends 18 U.S.C. § 2703[60] to allow a court, having jurisdiction over an offense, to issue a search warrant for stored data (e-mail) anywhere in the United States. Thus, a court in Virginia can issue a search warrant for records of a Michigan resident that reside on a California server.

Section 212[61] amends 18 U.S.C. § 2702 and § 2703, and allows Internet Service Providers to disclose information, with greater freedom, in two significant ways. Prior law had no provision for emergency disclosures, so if an ISP learned of a plan by one of its subscribers to perform an act of terrorism, the ISP could be civilly liable for disclosing that information. Section 212 resolves this by allowing, but not requiring, an ISP to disclose content and other information when it "reasonably believes" that there is an emergency that involves the immediate danger of "death or serious physical injury to any person."[62] The section also allows

---

[58] *Id.*

[59] Entitled "Nationwide Service of Search Warrants for Electronic Evidence."

[60] Entitled "Stored Wire and Electronic Communications and Transactional Records Access" - "Required Disclosure of Customer Communications or Records."

[61] Entitled "Emergency Disclosure of Electronic Communications to Protect Life and Limb."

[62] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56,

the ISP to disclose content and non-content information for purposes of self-protection. Under prior law, an ISP could disclose content to protect its rights and property, but could not disclose non-content, such as log-in records.

C. The Pen Register and Trap and Trace Statute

The Pen Register and Trap and Trace Statute[63] was written to regulate the interception of numbers dialed, received, or otherwise transmitted on a telephone line to which the information-gathering device is attached. However, the statute included only telephone technology when it was drafted. The privacy intrusion of this non-content information is considered to be lower than for content or for a wiretap. Thus, the statute was written to require a court to approve the request if law enforcement certified that the information is relevant to an ongoing investigation. Because the statute was originally written for telephones, section 216[64] of the PATRIOT Act amends the Pen Register and Trap and Trace Statute to make the provisions apply to Internet communications. Section 216 has the potential to be one of the broadest changes to prior law, and may have the most long-term effect of Title II, given the increasing importance of the Internet for communications. It makes three significant changes to prior law. First, the amendments to the ECPA clarify that the pen/trap statutes apply to Internet and other computer network traffic, provided that the devices do not include the contents of communications. The information may be any non-content information, including all "dialing, routing, addressing, and signaling technology."[65] The section also allows for a device or an "intangible process" to be "attached or applied to the target facility."[66] This provides clear

---

115 Stat. 272 § 212.

[63] 18 U.S.C. §§ 3121–27 (2000).

[64] Entitled "Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices."

[65] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 216.

[66] *Id.*

authority to use software instead of just physical mechanisms. Second, the section allows courts to issue orders that are valid anywhere in the United States, not just their own jurisdiction.[67] This recognizes the deregulation of communications providers and avoids the necessity to seek multiple supporting orders. Thus, an ISP may be presented with an order from a court outside its own state and which does not name the ISP specifically. Accordingly, there are protections that recognize this potential for confusion. The ISP has a right to receive "written or electronic certification"[68] from the law enforcement agency that the order applies to the ISP, and 18 U.S.C. § 3124(d) is amended to provide that an ISP's compliance with an order makes the ISP eligible for statutory immunity.[69] Third, if the ISP is unable to gather the information requested by its own capabilities and the FBI installs its DCS-1000 (Carnivore) or another device, it must then make a report to the court concerning the installation, configuration, and information collected.[70]

D. The Foreign Intelligence Surveillance Act of 1978

The Foreign Intelligence Surveillance Act of 1978 ("FISA")[71] allows the wiretapping, in the United States, of aliens and U.S. citizens, in circumstances of "foreign intelligence" rather than ordinary law enforcement.[72] The purposes of foreign intelligence collection are to deter, neutralize, or exploit espionage, sabotage, terrorism, and related hostile intelligence activities.[73] There must be a finding of probable cause to believe that the target of the wiretapping is a member of a foreign terrorist organization

---

[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] 50 U.S.C. §§ 1801–29 (2000).
[72] *See generally In re* Sealed Case No. 02-001 (Foreign Intell. Surveill. Ct. Rev. 2002) (Nov. 18, 2002).
[73] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 216.

or an agent of a foreign power.[74] If the target is a U.S. citizen or a resident alien, there must also be probable cause that the person is engaged in activities that may involve criminal violations. A secret FISA federal court hears the applications for wiretap orders. section 204 of the PATRIOT Act[75] explicitly excludes foreign intelligence operations from the criminal procedure protections of the ECPA, and reaffirms that FISA is the sole authority by which foreign intelligence electronic surveillance and interception of domestic wire and electronic communications may be conducted.[76]

One of the most controversial provisions of the PATRIOT Act is section 206,[77] which amends 50 U.S.C. § 1805 and expands the authority of FISA court orders to allow roving surveillance similar to ECPA roving wiretaps. Now, all wire or electronic communications relating to the investigation will be subject to the order, regardless of the suspect's location. This section is an attempt to thwart the use of disposable cell phones, changing e-mail accounts, and the use of multiple phone locations. A roving wiretap authority need not even name the individual or the entity that is being required to assist. Given the broadness of such an order, the PATRIOT Act provisions have several "good faith" compliance immunity provisions. Among the protections are the provisions in section 225[78] that provide immunity for "any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA.[79]

FISA can also authorize pen/trap requests. PATRIOT Act

---

[74] *Id.*

[75] Entitled "Clarification of Intelligence Exceptions from Limitation on Interception and Disclosure of Wire, Oral, and Electronic Communications."

[76] There are, however, additional rules for foreign intelligence surveillance. Executive Order No. 12333 (1982) addresses the ability of intelligence agencies to target U.S. citizens outside the United States, because there are no legislative restrictions on wiretaps or other electronic surveillance performed outside the United States. The order places limits on information gathered on U.S. citizens, incidental to intelligence gathering.

[77] Entitled "Roving Surveillance Authority Under The Foreign Intelligence Surveillance Act of 1978."

[78] Entitled "Immunity for Compliance with FISA Wiretap."

[79] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 206.

section 214[80] amends FISA at 50 U.S.C. § 1842(c)(3) and makes the requirements for pen/trap the same as the requirements of the ECPA. Thus, the requirement for obtaining a FISA pen/trap order now is a certification that the information to be obtained would be "relevant to an ongoing investigation."[81] This makes it easier to obtain a pen/trap order under FISA.[82] The section does, however, prohibit use of pen/trap in any investigation to protect against international terrorism or surveillance where the person has been singled out for investigation "solely on the basis of" First Amendment activities.[83]

Section 215[84] greatly expands the type of information that may be subject to a FISA request for records and has created considerable concern, especially for librarians whose ability to

---

[80] Entitled "Pen Register and Trap and Trace Authority Under FISA."

[81] *Id.*

[82] *See* Center for Democracy and Technology, E-Commerce & Privacy Group, *Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001, at* http://www.cdt.org/security/011031summary.shtml (Oct. 31, 2001) (on file with the North Carolina Journal of Law & Technology).

> Section 214: Pen register and trap and trace authority under FISA. Bottom Line: Expansion of FISA pen register/trap and trace authority in FISA that should lead to a significant increase in such requests. Makes it easier for the government to obtain a court order under FISA for pen register or trap and trace surveillance. Eliminates the requirement in 50 U.S.C. § 1842(c)(3) 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, Section 214 makes the FISA pen register/trap & trace requirements more closely track ECPA's requirements for such surveillance (i.e., providing a certification that the information obtained would be relevant to an ongoing investigation).

Id.

[83] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 206.

[84] Entitled "Access to Records and Other Items Under The Foreign Intelligence Surveillance Act."

protect patron privacy is seen to be eroded.[85] 50 U.S.C. § 1862 had limited FISA requests for business records to a narrow set of items.[86] Section 215 eliminates the categories and allows orders for business records to be issued to any person, including ISPs. Librarians and university press associations became extremely vocal about the effect on patron privacy, and section 215 has become a central point of the debate on the PATRIOT Act.[87]

---

[85] American Library Association, *Analysis of The USA Patriot Act Related to Libraries*, *at* http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/Intellectual_Freedom3/Intellectual_Freedom_Issues/The_USA_Patriot_Act_in_the_Library.htm (Apr. 2002) (on file with the North Carolina Journal of Law & Technology).

> Section 215: Access to Records Under Foreign Intelligence Security Act (FISA)
>
> - Allows an FBI agent to obtain a search warrant for "any tangible thing," which can include books, records, papers, floppy disks, data tapes, and computers with hard drives;
> - Permits the FBI to compel production of library circulation records, Internet use records, and registration information stored in any medium;
> - Does not require the agent to demonstrate "probable cause," the existence of specific facts to support the belief that a crime has been committed or that the items sought are evidence of a crime. Instead, the agent only needs to claim that he believes that the records he wants may be related to an ongoing investigation related to terrorism or intelligence activities, a very low legal standard;
> - Libraries or librarians served with a search warrant issued under FISA rules may not disclose, under of penalty of law, the existence of the warrant or the fact that records were produced as a result of the warrant. A patron cannot be told that his or her records were given to the FBI or that he or she is the subject of an FBI investigation;
> - Overrides state library confidentiality laws protecting library records.

Id.

[86] Center for Democracy, *supra* note 82. "Previously, section 501 of FISA (50 U.S.C. § 1862) had subjected only common carriers, public accommodation facilities, physical storage facilities, or car rental facilities to FISA business record authority." *Id.*

[87] *See* Dahlia Lithwick & Julia Turner, *A Guide to the Patriot Act, Part 1, Should you be scared of the Patriot Act*, SLATE (Sept. 8, 2003), *at* http://slate.msn.com/id/2087984/ (on file with the North Carolina Journal of

Attorney General John Ashcroft responded to the criticism by the American Library Association ("ALA"), other library associations, and civil rights protection groups by calling the concerns "baseless hysteria."[88] ALA President Carla Hayden issued a response to the Attorney General's remarks reaffirming the duty to protect patron privacy.[89] Attorney General Ashcroft then responded by calling

---

Law & Technology).

> Section 215 is one of the surprising lightning rods of the Patriot Act, engendering more protest, lawsuits, and congressional amendments than any other. In part this is because this section authorizes the government to march into a library and demand a list of everyone who's ever checked out a copy of My Secret Garden but also because those librarians are tough.

Id.

[88] Attorney General John Ashcroft, Department of Justice, *The Proven Tactics in the Fight against Crime*, Remarks at Meeting of National Astronaut Association (Sept. 15, 2003), *at* http://www.usdoj.gov/ag/speeches/2003/091503nationalrestaurant.htm (last visited Apr. 30, 2004) (on file with the North Carolina Journal of Law & Technology).

> Unfortunately, at this moment, Washington is involved in a debate where hysteria threatens to obscure the most important issues. If you were to listen to some in Washington, you might believe the hysteria behind this claim: "Your local library has been surrounded by the FBI." Agents are working round-the-clock. Like the X-Files, they are dressed in raincoats, dark suits, and sporting sunglasses. They stop patrons and librarians and interrogate everyone like Joe Friday. In a dull monotone they ask every person exiting the library, "Why were you at the library? What were you reading? Did you see anything suspicious?"
>
> According to these breathless reports and baseless hysteria, some have convinced the American Library Association that under the bipartisan Patriot Act, the FBI is not fighting terrorism. Instead, agents are checking how far you have gotten on the latest Tom Clancy novel.

Id.

[89] ALA President Carla Hayden, American Library Association, *American Library Association responds to Attorney General remarks on librarians and USA PATRIOT Act* (Sept. 16, 2003), *at* http://www.ala.org/Template.cfm?Section=News&template=/ContentManagement/ContentDisplay.cfm&ContentID=43916 (on file with the North Carolina Journal of Law & Technology).

Carla Hayden and offering his support declassifying the Justice Department's report on use of section 215.[90] ALA President Haden also stated:

> The ALA has been vocal on the issues of patron confidentiality and the protection of privacy. The library community stands ready to continue to participate in this important public debate and to seek the accountability and oversight necessary so that we can both counter terrorism and preserve our democracy's great strengths.[91]

The Justice Department revealed that it had never used section 215 to attempt to obtain library records.[92] Regardless of

---

> We are deeply concerned that the Attorney General should be so openly contemptuous of those who seek to defend our Constitution. Rather than ask the nations' librarians and Americans nationwide to "just trust him," Ashcroft could allay concerns by releasing aggregate information about the number of libraries visited using the expanded powers created by the USA PATRIOT Act.

Id.

[90] American Library Association, *ALA President welcomes call, commitment from U.S. Attorney General to declassify some PATRIOT Act reports* (Sept. 17, 2003), *at* http://www.ala.org/Content/ContentGroups/Press_Releases2/Press_Releases_2003_September/ALA_President_welcomes_call,_commitment_from_US_Attorney_General.htm (on file with the North Carolina Journal of Law & Technology).

> Today, American Library Association (ALA) President Carla Hayden welcomed a telephone call from U.S. Attorney General John Ashcroft. In the call, the Attorney General expressed his concern that people have misunderstood his commitment to civil liberties and committed to declassify the Justice Department report on Section 215 of the USA PATRIOT Act.

Id.

[91] *Id.*

[92] *See* International Association of Campus Law Enforcement Administrators, *at* http://www.iaclea.org/wmd/215AGmemo.htm (last visited Mar. 29, 2004) (on file with the North Carolina Journal of Law & Technology).

> Attached, for your information, is a memorandum from Attorney General Ashcroft to FBI Director Mueller regarding his decision to declassify the number of times Section 215 (business records provision—often referred to as the "library

whether section 215 is essential to fight terrorism, or whether the

---

provision") has been used. That number is ZERO (0). This provision has been the subject of a great deal of interest. A relevant article is also included below.

Jamie Brown
Director and Advisor to the Attorney General
Office of Intergovernmental and Public Liaison
United States Department of Justice
950 Pennsylvania Avenue, N.W.; Room 1629
Washington, DC 20530

MEMORANDUM FOR DIRECTOR ROBERT S. MUELLER

FROM: THE ATTORNEY GENERAL

SUBJECT: PATRIOT ACT SECTION 215

This memorandum confirms I have declassified the number of times to date the Department of Justice, including the Federal Bureau of Investigation (FBI), has utilized Section 215 of the USA PATRIOT Act relating to the production of business records. The number of times Section 215 has been used to date is zero (0).

I know you share my concern that the public not be misled regarding the manner in which the U.S. Department of Justice, and the FBI in particular, have been utilizing the authorities provided in the USA PATRIOT Act. Public confidence in law enforcement is of paramount importance. That is why I have taken this action despite the fact that it is generally not in the interest of the United States to disclose information of this nature.

While Congress has regularly been informed regarding the number of times Section 215 has been used, and while individual Members of Congress have been able to review that information, to date we have not been able to counter the troubling amount of public distortion and misinformation in connection with Section 215. Consequently, I have determined that it is in the public interest and the best interest of law enforcement to declassify this information.

Id.

PATRIOT Act was, for the most part, enactment of a "wish list"[93] for law enforcement, it certainly exemplifies the value of open public debate. The public debate also helped expose the use of "National Security Letters" by the Justice Department.[94]

Because section 215 broadens the scope of information that can be requested, section 215(e) creates immunity for good faith disclosures of business records and does not waive any other privilege. The authority cannot, however, be used for investigations of "United States Persons" being investigated solely on First Amendment activities.[95] The section also requires the Attorney General to report to Congressional committees on the use of the new authority.[96]

The duration of a FISA surveillance depends on many factors, including the nature, type, and importance of the information. Section 207[97] increased the initial duration of FISA surveillance to 120 days, and extensions can be requested.

Section 218[98] has also created great concerns with civil liberties watch groups. This section lowers the standard for FISA surveillance. A certification need only be made that "*a significant purpose*" rather than "*the purpose*" of surveillance or a search is to obtain foreign intelligence information. Thus, FISA will be able to collect criminal activity information as well as foreign intelligence.

---

[93] *See, e.g.*, ACLU, *ACLU Calls White House Report on Internet Crime Law Enforcement "Wish List"* (Mar. 9, 2000), *at* http://www.aclu.org/Privacy/Privacy.cfm?ID=7862&c=130 (on file with the North Carolina Journal of Law & Technology).

[94] *See* Dan Eggen & Robert O'Harrow, Jr., *U.S. Steps Up Secret Surveillance FBI, Justice Dept. Increase Use of Wiretaps, Records Searches*, WASH. POST, Mar. 24, 2003, at A01; *see also* VOWELL, *supra* note 7.

[95] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 215.

[96] *Id.*

[97] Entitled "Duration of FISA Surveillance of Non-United States Persons Who Are Agents of a Foreign Power."

[98] Entitled "Foreign Intelligence Information."

E. The Cable Act

The Cable Act[99] contains protections for subscriber information. It provides that a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned, and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator. The Communications Act provisions relating to cable are amended by section 211[100] to have the ECPA, the wiretap statute, and the trap and trace statue govern the release of information relating to Internet and telephone services by cable companies. When the Cable Act was adopted in 1984, cable companies were not providing telephone and Internet services. The Cable Act had very strict provisions regarding the release of personal information so that requests for data about Internet or phone customers required the cable provider to notify the customer before complying with the request for information. This amendment makes the release of relevant customer information consistent with other sources. Note, however, that the release of information concerning a customer's programming choices is still governed under the Cable Act.

F. The Federal Rules of Criminal Procedure

The Federal Rules of Criminal Procedure govern the procedures in all criminal proceedings in federal courts. The rules declare that they "are intended to provide for the just determination of every criminal proceeding."[101] By amending the Federal Rules of Criminal Procedure (Rule 6) and 18 U.S.C. § 2517, the PATRIOT Act section 203[102] permits intelligence information obtained in grand jury proceedings and from wiretaps to be shared with any federal law enforcement, protective, intelligence, immigration, and national defense individuals. Any intelligence

---

[99] 47 U.S.C. § 551 (2000).
[100] Entitled "Clarification of Scope."
[101] FED. R. CRIM. P. 2.
[102] Entitled "Authority to Share Criminal Investigative Information."

sharing is limited, however, to use in connection with the agent's official duties and subject to existing disclosure limitations. Grand Jury information also must be provided to the court after disclosure.

PATRIOT Act section 219[103] has significantly changed the law concerning search warrants. Under prior law, Rule 41(a) of the Federal Rules of Criminal Procedure required a search warrant to be obtained in the district where the search was to be made, and the only exception was if the property or person might leave the district before the warrant was executed. Section 219 amends that Rule and provides that, in domestic or international terrorism cases, a search warrant may be issued from anywhere in the United States in which activities related to terrorism have occurred.

Section 213[104] broadens the potential use of "sneak-and-peek" searches, i.e., surreptitious searches performed without notice.[105] Section 213 amends 18 U.S.C. § 3103 and allows the courts to delay the notice requirement to a "reasonable time" where there is reasonable cause to believe that providing immediate notice would have an "adverse result" or otherwise jeopardize an investigation or delay a trial.[106] The section is designed primarily for searches rather than seizures. A warrant issued must prohibit any seizure of tangible property or wire or stored electronic communication, unless the court finds "reasonable necessity" for the seizure.[107]

G. Additional Significant Title II Provisions

The PATRIOT Act specifies that there are no requirements to make any changes in existing technology by adopting section 222.[108] In 1994, Congress adopted the Communications

---

[103] Entitled "Single-Jurisdiction Search Warrants for Terrorism."
[104] Entitled "Authority for Delaying Notice of the Execution of a Warrant."
[105] *But see supra* note 5.
[106] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 203.
[107] *Id.*
[108] Entitled "Assistance to Law Enforcement Agencies."

Assistance for Law Enforcement Act ("CALEA" or "the digital telephony law").[109] CALEA was intended to preserve law enforcement wiretapping capabilities by requiring telephone companies to design their systems to ensure a certain basic level of government access. Section 222 relieves the provider of wire or electronic communication service of any additional requirements to provide technical assistance (such as with CALEA), furnish facilities, or require reconfigurations to allow surveillance. In addition, the section provides for reasonable compensation to the service provider for compliance with surveillance orders.

Section 223[110] increases civil liability for unauthorized disclosure of information gathered according to the PATRIOT Act and provides administrative discipline for federal officers or employees who engage in unauthorized disclosures.

Section 224[111] terminates the provisions of Title II on December 31, 2005. However, the exceptions to the sunset provisions are long and include many of the most controversial sections.[112]

---

[109] 47 U.S.C. §§ 1001–10 (1994).

[110] Entitled "Civil Liability for Certain Unauthorized Disclosures."

[111] Entitled "Sunset."

[112] The list of exceptions include:

- Section 203(a), which broadens authority to share grand jury information;
- Section 203(c), which establishes procedures regarding sharing of criminal investigative information;
- Section 205, employment of translators to support counterterrorism;
- Section 208, designation of FISA judges;
- Section 210, which broadens the scope of subpoenas for electronic communications service providers to include the disclosure of the means and source of payment;
- Section 211, which makes cable companies that provide Internet services the same as other ISPs and telecommunications providers;
- Section 213, which broadens the authority to delay notification of search warrants;
- Section 216, which extends trap and trace non-content to Internet traffic;
- Section 219, which allows single-jurisdiction search warrants for terrorism;
- Section 221, the trade sanction amendments; and

IV. Foreign Student Monitoring

Section 416[113] accelerates and expands the full implementation of the foreign student visa-monitoring program of the Illegal Immigration Reform and Immigrant Responsibility Act.[114] Full implementation was to be accomplished by January 1, 2003, and covers all nonimmigrant foreign students of all nationalities in covered foreign exchange programs and will include monitoring by any other approved educational institution. The INS (now the U.S. Citizenship and Immigration Services ("USCIS")) was directed to implement the Student Exchange Information System ("SEVIS"), an electronic tracking system.[115] The Family Educational Rights and Privacy Act ("FERPA")[116] does not apply to the information collected under SEVIS.[117]

- Section 222, which eliminates the imposition of technical obligations on a wire or electronic communication service provider.

[113] Entitled "Foreign Student Monitoring."

[114] 8 U.S.C. § 1372(a) (2002).

[115] The information to be collected will include:

- The current identity and address of the alien;
- The nonimmigration classification and the date the visa was issued or classification changed or extended or the date the change in classification was approved by the Attorney General;
- The current academic status, including whether the alien is maintaining full-time status or satisfying the terms and conditions of the program;
- Any disciplinary action taken by the institution as a result of a conviction for a crime, or change in participation as a result of the conviction of a crime; and
- The date of entry and port of entry of the alien.

[116] 20 U.S.C. § 1232g; 34 C.F.R. § 99 (2003).

[117] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 §§ 507 (entitled "Disclosure of Educational Records") and 508 (entitled "Disclosure of Information from NCES Surveys") amend the Family Educational Rights and Privacy Act and the confidentiality requirements of student databases to allow disclosure to the Attorney General or his designee, in connection with the investigation or prosecution of terrorism crimes. The PATRIOT Act provides immunity for good faith disclosure of records in response to an order.

V. Title VIII Expansion of Crimes and Penalties

The definitions of terrorism and terrorist acts have been changed and new offenses have been added.[118] The new crimes of harboring terrorists[119] and giving material support[120] have been added. The crime of harboring a terrorist is a ten-year felony for anyone who has "reason to know" that the person they are harboring has committed or is about to commit a terrorist act. The crime of giving material support is somewhat more problematic for colleges and universities. This new crime prohibits an organization from giving any kind of assistance to an individual who has been designated a "terrorist." There is no requirement that the assistance be intentionally given. Higher education generally gives the members of its community cash assistance, lodging, access to communications, and access to research equipment as a matter of course.

The PATRIOT Act has also created a new crime of "domestic terrorism."[121] Domestic terrorism is defined as "acts that are dangerous to human life, which appear intended to intimidate civilians or influence the policy of a government by intimidation or coercion or interfere with government operations by mass destruction, assassination, or kidnapping."[122] The vagueness of this new definition has concerned many with its potential application to acts of civil disobedience unrelated to terrorism.[123]

---

[118] The PATRIOT Act also expands the ability to designate a group as a terrorist group and expands terrorist crimes. *Id.* § 411.

[119] *Id.* § 803 (entitled "Prohibition Against Harboring Terrorists").

[120] *Id.* § 805 (entitled "Material Support for Terrorism").

[121] *Id.* § 802 (entitled "Definition of Domestic Terrorism").

[122] *Id.*

[123] *See* ACLU, *How The USA-Patriot Act Would Convert Dissent Into Broadly Defined "Terrorism,"* Oct. 23, 2001, *at* http://archive.aclu.org/congress/1102301d.html (on file with the North Carolina Journal of Law & Technology); Department of Justice, Dispelling the Myths Dispelling Some of the Major Myths about the USA PATRIOT Act, *at* http://www.lifeandliberty.gov/subs/u_myths.htm (last visited on Mar. 29, 2004) (on file with the North Carolina Journal of Law & Technology); *see also* Kathleen McFadden, *Ashcroft And Wilson Linked In National Media, Articles Question Anti-Terrorism Charges For "Common Crimes,"* (Sept. 25, 2003), *at* http://www.mountaintimes.com/

The expanded definition of the federal crime of terrorism includes unauthorized computer access to sensitive government information and dissemination of viruses.[124] Computer crimes are also greatly expanded to enhance the government's authority to prosecute hacking, cracking, and denial of service attacks.[125] The PATRIOT Act also clarifies and broadens the meaning of damage or loss under the Computer Fraud and Abuse Act,[126] and precludes private lawsuits for negligent design and manufacture of software and hardware. The PATRIOT Act also adds new defenses to civil or criminal liability under the ECPA for service providers who preserve stored data at the request of law enforcement officials.[127]

Biological and chemical agents are also addressed in the PATRIOT Act. Section 817[128] expands the restrictions on the possession and use of biological agents and toxins. Prior biological weapons law prohibited the possession, development, and acquisition of biological agents or toxins "for use as a weapon."[129] The PATRIOT Act amends the definition of "for use as a weapon" to include situations where it can be proven that the person had any purpose other than a prophylactic, protective, bona fide research, or other peaceful purpose.[130] The PATRIOT Act

---

mtweekly/2003/0925/ashcroft_wilson.php3 (on file with the North Carolina Journal of Law & Technology). The link between the two men—Watauga County District Attorney Jerry Wilson and U.S. Attorney General John Ashcroft—may not be immediately obvious aside from the fact that they're both lawyers and both prosecutors, but the two have been mentioned in the same news article at least twice before this one. A July 29 article in The Village Voice and a September 15 Associated Press article datelined Philadelphia draw parallels between the two men's use of anti-terrorism statutes to prosecute what the AP story calls "people charged with common crimes."

[124] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 808.

[125] *Id.* § 814 (entitled "Deterrence and Prevention of Cyberterrorism").

[126] 18 U.S.C. § 1030 (2000).

[127] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 815 (entitled "Additional Defenses to Civil Actions Relating to Preserving Records in Response to Government Requests").

[128] Entitled "Expansion of the Biological Weapons Statute."

[129] 18 U.S.C. § 175.

[130] The Uniting and Strengthening America by Providing Appropriate Tools

also creates an additional offense of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose.[131]

The PATRIOT ACT creates a new crime that makes it an offense for certain "Restricted Persons" to possess biological agents or toxins listed as a "select agent" by the Secretary of Health and Human services.[132] These provisions have been expanded and clarified in the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.[133]

Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 § 817.

[131] *Id.*

[132] 18 U.S.C. § 175b. Restricted persons include any individual who:

- Is under indictment for a crime punishable by imprisonment for a term exceeding 1 year;
- Has been convicted of a crime punishable by imprisonment for a term exceeding 1year;
- Is a fugitive from justice;
- Is an unlawful user of any controlled substance;
- Is an alien illegally or unlawfully in the United States;
- Has been adjudicated as a mental defective or has been committed to any mental institution;
- Is an alien (other than an alien lawfully admitted for permanent residency) who is a national of a country to which the Secretary of State has made a determination has repeatedly provided support for acts of international terrorism (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria); and
- Has been discharged from the Armed Services of the United States under dishonorable conditions.

Id. The CDC and APHIS have produced a list of select agents and toxins, which can be found on the CDC website at http://www.cdc.gov/ or on the APHIS website at http://www.aphis.usda.gov/ (on file with the North Carolina Journal of Law & Technology).

[133] Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), Pub. L. No. 107-188, 116 Stat. 594 (codified as amended in scattered sections of 42 U.S.C. and 21 U.S.C.). The Bioterrorism Act significantly changes the landscape of research regulation by requiring that individuals involved with select agents be investigated. Prior to enactment of the Bioterrorism Act, background checks were uncertain—with many universities engaging in their own. The Bioterrorism Act now places the burden of background checks on the Federal Government. The Bioterrorism Act also

VI. Conclusion: Responding to the USA PATRIOT Act

For institutions of higher education, the response to the PATRIOT Act must reflect the concerns for both the individual and the community good. On a theoretical level, members of the higher education community must be encouraged to engage in the debate on privacy versus surveillance. Institutions of higher education are unmatched in forcing difficult and unpopular opinions into the stream of social consciousness.[134] Moreover, academic freedom is an apt tool to examine the PATRIOT Act; to determine whether the Act is a reaction to a perceived security crisis, a necessary set of tools to thwart terrorism, or something in between. Regardless of where one stands on the surveillance debate, it must be acknowledged that the "shabby treatment civil liberties have received in the United States during times of war and perceived threats to its national security"[135] is a very real legacy of reaction, rather than response. It must equally be acknowledged that the current Justice Department believes in the necessity for "technological tools to anticipate, adapt, and outthink our terrorist enemy."[136]

On the practical side, higher education must respond as a

---

expands the reach of the PATRIOT Act's restricted persons prohibition to include those who are reasonably suspected by any federal law enforcement agency or intelligence agency of committing a crime of terrorism, knowing involvement in terrorism or an organization of terrorism, or being an agent of a foreign power.

[134] *Cf. Hearing on Antiterrorism Policy before the Senate Comm. on the Judiciary*, 106th Cong. (2001) (statement of Attorney General John Ashcroft).

> We need honest, reasoned debate; not fearmongering. To those who pit Americans against immigrants, and citizens against non-citizens; to those who scare peace-loving people with phantoms of lost liberty; my message is this: Your tactics only aid terrorists—for they erode our national unity and diminish our resolve. They give ammunition to America's enemies, and pause to America's friends. They encourage people of good will to remain silent in the face of evil.

Id.

[135] Brennan, *supra* note 6.

[136] Baker, *supra* note 10.

law-abiding citizen, with the knowledge that a very real threat has presented itself and with the understanding that the threat must be faced. Each institution must examine what privacy it is "promising" its community members and must also decide what it can actually deliver in light of the new demands for surveillance. The establishment of protocols, procedures, and routines for surveillance requests will benefit all involved and following a general routine can prevent mistakes and unauthorized disclosures;[137] many wiretap orders, warrants, and subpoenas have specific provisions for not revealing the surveillance or information production and now may not specify the exact information to be disclosed.[138] For Information Technology ("IT") administrators, it is essential to establish emergency and computer trespasser procedures. The PATRIOT Act allows disclosure of content and other material if there is an emergency situation. IT administrators must make an informed decision how to respond on this issue. Considering how this may relate to the new crime of assisting a terrorist, situations cannot simply be ignored. Similarly, hacking and cracking attempts should be reported so that a decision can be made whether law enforcement will be involved in computer trespasser activities.

The Justice Department, U.S. Citizenship and Immigration Services, and National Security Agencies have been challenged to perform an extraordinarily difficult task, one that puts the basic struggle of individual freedoms and public good at issue. This

---

[137] It is important to take students, clerks, and others out of the information release process, to prevent disclosures or confidentiality breaches. Many court orders, warrants, and subpoenas prohibit disclosure to the target or others. The consequences of unauthorized disclosure could be disastrous. It is unfair to expect confidentiality from those who were not hired to maintain it. Neither is it fair to expect students or clerical employees to make decisions on whether or how to release information.

[138] Warrants, orders, subpoenas, and other requests are often written in "law-enforcement-ese" and "legal-ese." Counsel can help translate the exact requests and demands that are being made. This will help to prevent over-inclusion or under-inclusion in the production of information. In addition, counsel can work with the requesting agency and campus departments for an efficient and restricted production or surveillance. Counsel can also coordinate the duties and responsibilities imposed by other laws, policies, and procedures and help maintain confidentiality and privacy rights.

philosophical struggle has already erupted on campus, and the causes of that philosophical struggle have become increasingly concrete because the new realities of the fight against terrorism have changed the way information is requested. Because administration, faculty, students, and staff will not all agree on what a reasonable expectation of privacy should be or the degree with which to cooperate with requests for surveillance or confidential information, higher education will be forced to make fundamental choices as to how it will balance the interests in the face of the new way of thinking, while being mindful of, and a key participant in, the debate between individual and community needs.