Higher Education Issues After The USA Patriot Act

David Lombard Harrison
Division of Legal Affairs
Office of the President
The University of North Carolina

I. THE PATRIOT ACT: A NEW WAY OF THINKING

A. 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 (the USA PATRIOT Act). The bill that created the Act was 342 pages long, had several significant changes in its final days, and will affect more than 15 already-existing statutes.

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. This paper primarily addresses provisions applicable to higher education.

B. Title II, Enhanced Surveillance Activities

Title II is 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? Title II's solution, which broadens the powers of law enforcement and national security agencies to conduct surveillance, will have a significant impact on campus technologies and will affect the privacy interests of everyone, both on campus and off.

Although Title II of the USA PATRIOT Act has received most press for the provisions concerning "roving wiretaps," "sneak-and-peek" warrants, Carnivore applications, lowered standards for gaining surveillance authority, and other technical issues, its less overt result is a fundamental shift in 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. As Jim McGee reported in The Washington Post, Sunday, November 4, 2001, Page A04, "An Intelligence Giant in the Making,"

> '"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."'

This "new way of thinking" will result in significant changes to all of our lives, including increases in both the scope and number of surveillance requests to college and university service providers – whether Internet, telecommunications, or cable. In fact, the Justice Department has reported that it began using the Act within hours of its enactment.

This paper is meant to familiarize the academic community with the existing surveillance laws, the basics of wire and electronic surveillance, and selected provisions of the USA PATRIOT Act, in order to prepare for this impending increase in demands for confidential information and surveillance.

C. Title IV Foreign Student Monitoring

Section 416 accelerates and expands the full implementation of the foreign student visa monitoring program of the Illegal Immigration Reform and Immigrant Responsibility Act, 8 USC 1372(a). Full implementation is to be accomplished by January 1, 2003 and will cover all nonimmigrant foreign students of all nationalities in covered foreign exchange programs. The INS will implement the Student Exchange Information System (SEVIS), which is an electronic tracking system.

Expansion of the Act will include the coverage of nonimmigrant students (F, J, and M) of all nationalities and will include monitoring by any other approved educational institution.

FERPA will not apply to the information collected under SEVIS.

D. Title V and FERPA Exceptions

Following September 11, nearly 300 requests were made for information under the health and safety emergency exceptions. Although most were honored, the PATRIOT Act provides for a new procedure to obtain an order for release of otherwise protected information.

E. Title VIII Bioterrorism Provisions

Section 817 expands the restrictions on the possession and use of biological agents and toxins to include situations where it can be proven that the person had any purpose other than a prophylactic, protective, and bona fide research, or other peaceful purpose.

This section also creates a new statute, 18 USC §175b, which 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. Restricted persons include an 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;
- In 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 as 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);
- Has been discharged from the Armed Services of the United States under dishonorable conditions.

II. SURVEILLANCE AND PRIVACY PERSPECTIVES

> 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.

United States Constitution, Amendment IV. The essence of the Fourth Amendment is that government cannot intrude when one has a reasonable expectation of privacy. Of course, the definition of what is "reasonable" is not static.

In response to the September 11 attacks, the USA PATRIOT Act brings the Fourth Amendment to the forefront of the national debate. Title II changes the relationship of a communications provider to those it serves and increases the power of law enforcement to perform surveillance and retrieve information. 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.
- Opens the door to allowing law enforcement to secretly install software on individual computers or deliver surveillance software by Trojan horse e-mails.

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.

The tensions that mark the debate between surveillance needs and the preservation of civil liberties have their roots in the fundamental struggle of community interests versus individual interests. This paper advances no opinion on the primacy of those interests, but the debate must be recognized, because the provisions of the USA 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 has already asked that the Act be strengthened and the use of computer key logging is already being challenged in the federal courts. Moreover, your institution must make a fundamental choice as to how you will balance the interests with your implementation of privacy and surveillance policies, in the face of new definitions of assisting terrorism and expansion of definitions of computer crimes.

The surveillance and privacy debate is not new. Henry Stimson is known for making one of the most memorable statements concerning the ethics of surveillance:

> After he entered the White House in 1933 he [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 codebreaking agency, famously declaring that `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 1930s. 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-1930s it was regularly cracking Japanese diplomatic ciphers. By the end of the decade these were being discreetly circulated in Washington under the codename `Magic'.

Stafford, David. Roosevelt and Churchill, Men of Secrets, The Overlook Press, 1999. It is interesting to note that the FBI just admitted to its own "Magic Lantern," which is a computer Trojan horse, surreptitiously delivered by e-mail, and capable of recording every keystroke of a computer.

It is certainly naïve to reject all surveillance as a necessary national tool, and many critics today blame the continued naivety in rules for intelligence gathering as a reason for the devastating success of the 9/11 operation. But, 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 in a paper delivered at the Law School of Hebrew University, in Jerusalem:

> 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 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.

William J. Brennan, Jr., Associate Justice, Supreme Court of the United States, *The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crises*, delivered at the Law School of Hebrew University, Jerusalem, Israel, December 22, 1987. His audience was certainly well aware of how civil liberties can be threatened in times of war and security crisis.

It is this philosophical backdrop that makes issues of surveillance and intrusions into privacy so close to the heart of American life, and which fuels the debate surrounding the USA PATRIOT Act. This philosophical struggle will also affect your privacy procedures, because your administration, faculty, students, and staff will not all agree on the same definition of "reasonable expectation of privacy" or the degree with which to cooperate with requests for surveillance or confidential information.

III. FREQUENTLY ASKED QUESTIONS ABOUT SURVEILLANCE AND THE PATRIOT ACT

A. General Effect on Colleges and Universities

1. How will the USA PATRIOT ACT affect my institution?

The provisions of the Act that relate to information held by an Internet Service Provider, telephone system operator, or cable provider have no exceptions for institutions of higher education. These sources have long been subject to wiretapping and other information requests under prior law and most institutions have at least some limited experience with law enforcement requests for information.

The new realities of terrorism, however, will change the way and frequency with which information is requested. Moreover, the usual methods in the past included

substantial periods of time to work with law enforcement requests. Now, it is more likely that there will be requests that must be acted upon immediately.

Title II of The USA PATRIOT Act's primary goal is to make information easier to get. Section 103 of the Act also specifically authorizes $600 million to the FBI's technical support center, over the next three years, and Section 208 increases the Foreign Intelligence Surveillance Act Court from 7 to 11 judges, which should result in significant additional surveillance activities and initiatives.

2. Why should colleges and universities specifically be concerned?

Today's colleges and universities have an unmatched intersection of high technology and foreign nationals – the primary concerns of the Act. Yet, institutions of higher learning are also constrained by various privacy laws and are frequently at the forefront of First Amendment and academic freedom issues. Thus, surveillance and monitoring will require institutions to carefully balance the competing needs.

In the weeks following 9/11, over 200 "emergency" requests were made to colleges and universities for release of information that would otherwise have been protected by FERPA. It is unlikely that many emergency requests have ever been made before. The USA PATRIOT Act is meant to facilitate continued wide-scale requests.

B. Methods of Surveillance and Information Gathering

1. Wiretapping and search warrants already exist, what is the USA PATRIOT Act intended to do?

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 USA PATRIOT ACT are a reaction to those advances in technology and infrastructure, and 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 every byte of data from every source and sort it.

2. What types of communication can be intercepted or gathered?

The law specifies three basic types of communication that can be gathered:

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. 18 USC §2510(2).

Wire communication is a human utterance transmitted in whole or in part over wire, cable, or similar connection furnished by a telecommunications facility, but did not

include the portion of a communication transmitted by a cordless telephone until 1994. 18 USC §2510(1).

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. 18 USC §2510(12).

3. How is information gathered?

There are three general methods of information gathering that are at issue with the PATRIOT Act. These are wiretaps, pen/trap devices, and Internet/computer gathering devices.

4. What is a wiretap?

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. 18 USC §2510(4). "Content" means any information concerning the substance, purport, or meaning of that communication. 18 USC §2510(8).

5. What are Pen Registers and Trap and Trace Devices (Pen/Trap)?

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. 18 USC §3127(3). A trap and trace device is a device attached to a telephone line, which records the number of each telephone dialing into that line. 18 USC §3127(4). They are treated identically in federal surveillance laws.

6. What are Carnivore (DCS-1000) and DragonWare Internet "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, which they are not authorized to intercept. Others, who have analyzed the system, state that DCS-1000 is part of a suite of tools (known as DragonWare) including Packeteer and Coolminer, and which can combine to recreate Web pages exactly as a surveillance subject saw them.

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 those packets with information is looking for. Because all information on the Internet travels in packets, some have challenged the "surgical" ability of DCS-1000.

7. What are Magic Lantern and Key Loggers?

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. It

is a Trojan horse (similar to a "virus") sent through e-mail and 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) and the use of key logging is currently being challenged in court. See, United States v. Scarfo, Criminal No. 00-404 (D.N.J.).

8. Who can collect the information from my institution?

The surveillance laws allow many different agencies to collect information. The agencies include all of the Department of Justice agencies (e.g., FBI, INS), 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.

It is very unlikely that states will use the Act, however, since most states have neither the resources nor inclination to investigate terrorism and they are constrained by their own surveillance laws, which can be more restrictive than the federal law.

Thus, the FBI or another Justice Department official will most likely approach you with a request for information, sometimes in cooperation with a state agency.

9. What notice will we receive that information is being sought?

You would receive an order, warrant, subpoena, or notification for preservation of information. 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. The manual is online and available at http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm. The CCIPS Appendix section contains examples of typical orders, warrants, and requests.

Generally, there is a "hierarchy" of difficulty in getting information.

- The lowest is the simple request, without any formal document. This may be for information that is public or readily available without an expectation of privacy, or is being provided with consent.

- A letter request is the next level. It will specify the information being sought. See, e.g., CCIPS Appendix C.

- A subpoena is the next level and, although it is a court document, a federal official, rather than a court issues it. See, e.g., CCPIS Appendix E.

- 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. See, e.g., CCPIS Appendix F.

- A pen/trap order is more difficult to obtain and contains very specific information. See, e.g., CCPIS Appendix D. 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. 18 USC §3123(b). 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. 18 USC §3122(2).

- A wiretap Order is the most difficult to obtain. 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, (5) the period of time during which interception is permitted and whether the interception must terminate when the communications sought are first obtained. 18 USC §2518(4).

  The order also must state that the interception (1) shall be executed 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. 18 USC §2518(5).

  There are unique circumstances where a law enforcement officer, specially designated by high-ranking Justice official, may authorize a wiretap without an order.

There are many exceptions to the notice and the procedural provisions, however, from consent to exigent circumstances and an order is not always required to collect information.

C. The PATRIOT Act's Significant Changes to Existing Surveillance Laws

1. What laws are changed by Title II of the PATRIOT ACT?

The PATRIOT Act affects many existing statutes and Orders. The actual language of many of the Act's sections is impossible to understand in isolation because much of the text simply references the other statutes. The statutes include, The Federal Wiretap Statute, 18 USC §2510 et. seq. (Title III), The Electronic Communications Privacy Act of 1986, 18 USC §2801 et. seq. (ECPA) which includes, for the purposes of this paper, The Stored Wire and Electronic Communications Act, 18 USC §2701 et. seq., The Pen Register and Trap and Trace Statute, 18 UCS §3121 et. seq., The Foreign Intelligence Surveillance Act of 1978, 50 USC §1801, et. seq. (FISA), Executive Order 12333 of 1982, The Cable Act, 47 USC §551, The Computer Fraud and Abuse Act 18 USC §1030, and The Federal Rules of Criminal Procedure (FRCrP).

D. Significant Changes To The Wiretap Law

1. What is The Federal Wiretap Statute, 18 USC §2510 et. seq. (Title III)?

The Federal Wiretap Act was enacted in 1968 and is often referred to as "Title III." 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 communications has been held to be the most serious of intrusions into the rights of privacy. A wiretap order for oral or wire communications may be issued only for specific serious felonies 18 USC §2516(a)-(p). A wiretap order to intercept electronic communications may be issued for any federal felony. 18 USC §2516(3).

Targets who have had their communications intercepted must be notified of the interceptions no later than 90 days after completion of the wiretaps.

2. Can I ask for help from law enforcement to stop hackers?

The wiretap statute allows 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, Interception Of Computer Trespasser Communication, allows (but does not require) an ISP to enlist the assistance of law enforcement, and protects the government from liability if it conducts warrantless wiretaps of computer trespassers. The trespasser's activity need not relate only to terrorism, however.

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." 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.

3. Can voice communication be intercepted in hacking investigations?

Section 202, Authority To Intercept Wire, Oral, Or Electronic Communications Relating To Computer Fraud And Abuse Offenses, Amends 18 USC §2516(1) allows a wiretap order to intercept wire communications (involving the human voice) for violations of the Computer Fraud and Abuse Act (18 USC §1030). This amendment will allow investigators to intercept online human voice transmissions when investigating hacking offenses.

E. Significant Changes To The ECPA

1. What is The Electronic Communications Privacy Act of 1986, 18 USC §2801 et. seq. (ECPA)?

The ECPA 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 email, but transactional records may be obtained by use of an administrative subpoena, which is much easier to obtain than a warrant.

2. Is a wiretap order required to turn over voicemail?

No. Section 209, Seizure Of Voicemail Messages Pursuant To Warrants, overturns case law, US v Smith, 155 F3d 1051 (9th Cir 1998), cert denied, and the ECPA, 18 USC §2510(1), which required law enforcement to seize voice mail messages with a wiretap order, rather than a search warrant. This amendment makes access to voicemail the same as for email.

3. What kinds of information can be released with a subpoena?

Section 210, Scope of Subpoena for Electronic Evidence, amends 18 USC §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."

These provisions are meant to make the provisions of 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 6 months and the government has followed the required procedures.

4. What courts can issue warrants for e-mails?

Section 220, Nationwide Service Of Search Warrants For Electronic Evidence, amends 18 USC §2703 to allow a court, having jurisdiction over an offense, to issue a search warrant for stored data (e-mail) anywhere in the United States. This means that you will not always be given a search warrant that has been issued in your district or state.

5. What can I do if I learn of a plan by one of my subscribers to cause death or serious injury?

Section 212, Emergency Disclosure Of Electronic Communications To Protect Life And Limb, amends 18 USC §2702 and §2703, 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."

The section also allows the ISP to disclose content and non-content information for purposes of self-protection. Under prior law, and ISP could disclose content to protect its rights and property, but could not disclose non-content, such as login records.

F. Significant Changes To The Pen Register And Trap And Trace Statute, 18 UCS §3121 Et. Seq.

1. What is The Pen Register and Trap and Trace Statute, 18 UCS §3121 et. seq.?

This statute was written to regulate the interception of numbers dialed, received, or otherwise transmitted on the telephone line to which the device is attached. The statute included only telephone technology when it was drafted. Because the privacy "intrusion" of this non-content information is lower than for content or for a wiretap, a court must approve the request if law enforcement certifies that the information is relevant to an ongoing investigation.

2. If the statute was written for telephones, can it apply to Internet communication?

It can now. Section 216, Modification Of Authorities Relating To Use Of Pen Registers And Trap And Trace Devices, has the potential to be the broadest change and have the most long-term effect of Title II. 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." The section also allows for a device or an "intangible process" to be "attached or applied to the target facility. This provides clear authority to use software instead of just physical mechanisms.

Second, the section allows the courts to issues orders that are valid anywhere in the United States, not just their own jurisdiction. This recognizes the deregulation of communications providers and avoids the necessity to seek multiple, supporting orders. This means that 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" from the law enforcement agency that the order applies to the ISP and 18 USC §3124(d) is amended to provide that an ISP's compliance with an "order" make the ISP eligible for statutory immunity.

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.

G. Significant Changes To The Foreign Intelligence Surveillance Act Of 1978, 50 USC §1801, Et. Seq. (FISA)

Q. What is FISA?

FISA allows the wiretapping, in the United States, of aliens and U.S. citizens, in circumstances of "foreign intelligence" rather than ordinary law enforcement. The purposes of foreign intelligence collection are to deter, neutralize, or exploit espionage, sabotage, terrorism, and related hostile intelligence activities.

There must be a finding of probable cause to believe that the target of the wiretapping is a member of a foreign terrorist organization or an agent of a foreign power. If the target is a U.S. citizen or a resident alien, there must also be a probable cause that the person is engaged in activities that may involve criminal violations.

A special, secret federal court hears the applications for wiretap orders.

2. Do FISA surveillance activities follow the same procedures as the ECPA or other criminal law?

No, Section 204, Clarification Of Intelligence Exceptions From Limitation On Interception And Disclosure Of Wire, Oral, And Electronic Communications, 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.

3. Will a FISA wiretap Order name the person and my institution?

Not necessarily. This is one of the most controversial provisions of the USA PATRIOT Act. Section 206, Roving Surveillance Authority Under The Foreign Intelligence Surveillance Act Of 1978, amends 50 USC §1805 and expands the authority of FISA court orders to allow roving surveillance similar to ECPA roving wiretaps. 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 email accounts, and the use of multiple phone locations.

A roving wiretap authority need not name the individual or the entity that is being required to assist.

4. How can we avoid liability for disclosure if we are not even named in the Order?

The FISA provisions have several "good faith" compliance immunity provisions. Among the protections are the provisions in Section 225, Immunity For Compliance With FISA Wiretap. This section provides broad immunity for "any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA.

5. Can FISA also authorize pen/trap requests?

Yes, Section 214, Pen Register And Trap And Trace Authority Under FISA, amends 50 USC §1842 (c)(3) and brings the requirements for pen/trap under FISA, in line with the requirements of ECPA. The requirements are lowered from specific certifications to certification that the information to be obtained would be relevant to an ongoing investigation. This makes it easier to obtain a pen/trap order under FISA.

The section also prohibits 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.

6. Can FISA authorize the use of a subpoena for records?

Yes. Section 215, Access To Records And Other Items Under The Foreign Intelligence Surveillance Act, greatly expands the type of information that may be subject to a FISA request for records. 50 USC §1862 had limited FISA requests for business records to a narrow set of items. Section 215 eliminates the categories and allows orders for business records to be issued to any person, including Internet Service Providers.

Because this broadens the scope of information that can be requested, §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. The section also requires the Attorney General to report to Congressional committees on the use of the new authority.

7. How long will FISA surveillance last?

This depends on many factors, including the nature, type, and importance of the information. The Act increased the initial duration of FISA surveillance to 120 days in Section 207, Duration Of FISA Surveillance Of Non-United States Persons Who Are Agents Of A Foreign Power, and extensions can be requested.

8. Is FISA only for foreign intelligence?

No. Section 218, Foreign Intelligence Information, has 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.

9. Are there other rules for foreign intelligence surveillance?

Yes, Executive Order 12333 of 1982 addresses the ability of intelligence agencies to target U.S. citizens outside the United States. 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 (including information collected by the "vacuum cleaner" methods, such as Echelon), incidental to intelligence gathering.

H. Significant Changes To The Cable Act, 47 USC §551

1. How is the Cable Act affected?

The Cable Act, 47 USC §551, contains provisions that protect subscriber information. They provide 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 services (The Cable Act, 47 USC §551) are amended by Section 211, Clarification Of Scope, 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.

I. Significant Changes To The Federal Rules Of Criminal Procedure (FRCrP)

1. What are 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."

2. Can one agency share information with another agency?

By amending Federal Rules of Criminal Procedure (Rule 6) and 18 USC §2517, Section 203, Authority To Share Criminal Investigative Information, Title II 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 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.

3. Will search warrants be issued from my own district?

Section 219, Single-Jurisdiction Search Warrants For Terrorism, has changed the law. 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 the 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.

4. Will the suspect always be notified before a search is conducted?

No, Section 213, Authority For Delaying Notice Of The Execution Of A Warrant, broadens the potential use of "sneak-and-peek" searches; i.e., surreptitious searches

performed without notice. Section 213 amends 18 USC §3103a 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. 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.

J. Additional Significant Title II Provisions

1. Do I have to make any changes to existing technology in order to comply with the USA PATRIOT Act?

No, Congress specifically determined that your institution does not have to make any changes by adopting Section 222, Assistance To Law Enforcement Agencies.

In 1994, Congress adopted the Communications Assistance for Law Enforcement Act (CALEA, or the digital telephony law). 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.

2. What if information is released in violation of the Act?

Section 223, Civil Liability For Certain Unauthorized Disclosures, increases civil liability for unauthorized disclosure of information gathered according to the Act and provides administrative discipline for federal officers or employees who engage in unauthorized disclosures.

3. Are all the changes permanent?

No, Section 224, Sunset, 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. 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.
- Section 222, which eliminates the imposition of technical obligations on a wire or electronic communication service provider.

This means that many of the changes will most likely be around for a long time.

IV. SECTION 416 FOREIGN STUDENT MONITORING

1. Will the INS Require Monitoring of Foreign Students?

Section 416 accelerates and expands the full implementation of the foreign student visa monitoring program of the Illegal Immigration Reform and Immigrant Responsibility Act, 8 USC 1372(a). Full implementation is to be accomplished by January 1, 2003 and will cover all nonimmigrant foreign students of all nationalities in covered foreign exchange programs. The INS will implement the Student Exchange Information System (SEVIS), which is an electronic tracking system.

Expansion of the Act will include the overage of nonimmigrant students (F, J, and M) of all nationalities and will include monitoring by any other approved educational institution.

FERPA will not apply to the information collected under SEVIS.

2. What information will be collected?

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;

- The date of entry and port of entry of the alien.

V. FERPA AND TITLE V CHANGES

1. Does the PATRIOT Act affect FERPA?

Yes, Sections 507 & 508 amend the Family Educational Rights and Privacy Act (FERPA) 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.

2. Are there any protections for disclosure?

Yes, the Act provides immunity for good faith disclosure of records in response to an order.

VI. TITLE VIII EXPANSION OF CRIMES AND PENALTIES

1. Has the definition of "terrorism" been changed?

The definition of terrorism and terrorist acts has been changed and new offenses have been added. The new crimes of harboring terrorists (§803) and giving material support (§805) have been added.

§803 is a 10 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.

§805 is somewhat more problematic for Colleges and Universities. This prohibits an organization from giving any kind of assistance (including, for example, cash assistance, lodging, communications equipment, facilities . . .) to an individual who has been designated a "terrorist." There is no requirement that the assistance be intentionally given. The Act also expands the ability (§411) to designate a group as a terrorist group, and expands terrorist crimes.

The Act has also created a new crime of "domestic terrorism," in §802.

2. What is the crime of Domestic Terrorism?

Section 802 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.

3. Can computer crimes be terrorism?

Yes. The Act includes unauthorized computer access to sensitive government information and dissemination of viruses in the expanded definition of the federal crime of terrorism. §808.

Computer crimes are also greatly expanded in §814, Deterrence And Prevention Of Cyberterrorism, which enhances the government's authority to prosecute hacking, cracking, and denial of service attacks, clarifies and broadens the meaning of damage or loss under the Computer Fraud and Abuse Act, and precludes private lawsuits for negligent design and manufacture of software and hardware.

4. Are there any new protections for an ISP that provides information under the Act?

Yes. Section 815, Additional Defenses To Civil Actions Relating To Preserving Records In Response To Government Requests, 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.

5. Are Biological And Chemical Agents Addressed In The Act?

Section 817 expands the restrictions on the possession and use of biological agents and toxins. Prior law, 18 USC §175, prohibited the possession, development, and acquisition, of biological agents or toxins "for use as a weapon." Section 817 amend 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, and bona fide research, or other peaceful purpose.

§817 also adds a subsection to 18 USC §175, which defines 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. This section also creates a new statute, 18 USC §175b, which 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.

6. Who are "Restricted Persons" under the Act?

Restricted persons include an 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;
- In 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 as 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);
- Has been discharged from the Armed Services of the United States under dishonorable conditions.

VII. RESPONDING TO THE USA PATRIOT ACT

A. Title II Surveillance and Monitoring

Although The USA PATRIOT Act concerns surveillance by the government, it is also appropriate that you review and harmonize your internal privacy policies for faculty, staff, and students with steps you will take in response to the Act. In this digital information age, it is appropriate that you don't create expectations of privacy that you simply cannot ensure. While Sun Microsystems CEO Scott McNealy's statement that "You have zero privacy, anyway. Get over it," may be extreme, no Internet Service provider or other provider of communications can guarantee privacy.

Any expectation of privacy on the Internet or Local Area Network should be replaced with a frank realization that privacy cannot be provided or promised to any user of Internet or network computer resources. 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. Your users should be aware of that.

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, your policies should address the limitations of access and interference, and the information release and disclosure protocols should protect unreasonable access and interference. In addition, users should be aware that the service provider adheres to all applicable laws that protect the members of the institution community – including the USA PATRIOT Act.

In order to comply with the new demands of the USA PATRIOT Act, certain procedures and policies are appropriate. For example:

- Establish a protocol for all information requests.

  It is likely that your Information Technology and Communications staff have been approached by your campus police, human resources, or others to gain access to information. Review what they do in response to the

requests and modify the practices to conform to privacy policies and the new concerns of the USA PATRIOT Act.

- Establish or modify privacy policies.

  If you have privacy policies, review them in light of the new demands for surveillance. See what you are "promising" your community and decide what you can actually deliver. If you do not have policies, establish them for all aspects of community life including computing, network, Internet, telecommunications, email, etc.

- Have a single point of entry for all information and surveillance requests.

  All IT and Communications staff should be made aware of who can actually release information and how. This will avoid the release of information from a relatively low-level employee. It will also provide a common person or office that can become familiar with the processes and procedures.

- Keep a confidential log of all information and surveillance activities.

  The USA PATIOT Act and other statutes have defenses and immunities for good faith compliance with official requests. Record what is requested, how it was provided, to whom, when, etc., and keep it confidential. This will help prevent accusations of wrongdoing and will "force" you to follow sound procedures.

- Establish routines for surveillance activities and requests.

  Following a general routine can prevent mistakes and unauthorized disclosures. Many wiretap orders, warrants, and subpoenas have specific provisions for not revealing the surveillance or information production, and for the exact type of information to be disclosed.

- Establish emergency and computer trespasser procedures.

  Make sure that all suspicious activity is reported promptly, accurately, and to a designated person or office. The USA PATRIOT Act allows disclosure of content and other material if there is an emergency situation. Teach your staff what that means and also make an administrative decision as to what position you are going to take on this issue. Consider how this relates to the new crime of assisting a terrorist.

  Similarly, hacking and cracking attempts should be reported so that the law enforcement option can be considered. Make an administrative

decision as to whether law enforcement will be involved in computer trespasser activities.

- Prevent disclosures or confidentiality breaches.

  Take students, clerks, and others out of the loop. It is unfair to expect confidentiality from those who were not hired to maintain it. Neither is it fair to expect students or lower level employees to make decisions on whether or how to release information. Many court orders, warrants, and subpoenas prohibit disclosure to the target or others. A criminal charge of obstruction of justice or the consequences of unauthorized disclosure could be disastrous.

- Know what to look for when a request is made.

  Talk to your local law enforcement and get to know what to expect. Review sample orders such as those in CCIPS, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm and become familiar with court documents.

- Conduct a capability study.

  The FBI won't use its Carnivore or other devices if your system can provide the information. You don't have to make any technical changes, but if you can accommodate the legal request, then be prepared to do so.

- Involve legal counsel in all requests for information.

  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 being made. This will help to prevent over-inclusion or under-inclusion. 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.

By taking the time to examine your privacy policies, you will be able to begin to identify what works and what doesn't on your campus.

B. Responding to §416 Foreign Student Monitoring

- Assess and determine the IT system in place and whether the system will be compatible with the INS program.

- Follow the additional bills in progress, such as Brownback Kennedy (S. 618), Feinstein Kyl (S. 1627), which may require addition certification, registration, training, affirmative background checks, and demonstrations of compliance and training.

C. Responding to §817 Bioterrorism Requirements

- Determine your current safety and security procedures. Who has access, when, how, and with what safeguards. Consider all "agents" at issue and be diligent in adding security to research activities.
- Background checks are not yet required, but consider them. A checklist for all persons with access is a good starting point.
- Inventory your chemical and biological agents.
- Review and publish the select agents list.
- Determine registration compliance.
- Create or enhance tracking systems.
- Enhance training for all lab personnel.
- Make disposal a recorded event.
- Train and retrain handling and access.

VIII. CONCLUSION

The Justice department, Immigration and Naturalization Service, and National Security Agencies have been challenged to perform an extraordinarily difficult task -- a task that involves the potential intrusion on the most basic privacy rights of your campus community members. Regardless of where you stand in the debate on community versus individual rights, a solid and well-established set of privacy, surveillance, hazardous materials handling, and information production procedures and protocols will ensure that you have taken most effective and least intrusive actions possible.