

## What is the Patriot Act?

### Answer:

The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (i.e., PATRIOT Act) was designed to broaden the surveillance capabilities of law enforcement. It includes ten "Titles":

Title I	Enhancing Domestic Security Against Terrorism
Title II	Enhanced Surveillance Procedures
Title III	International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001
Title IV	Protecting the Border
Title V	Removing Obstacles to Investigating Terrorism
Title VI	Providing For Victims of Terrorism, Public Safety Officers, and Their Families
Title VII	Increased Information Sharing for Critical Infrastructure Protection
Title VIII	Strengthening the Criminal Laws Against Terrorism
Title IX	Improved Intelligence
Title X	Other

Universities providing Internet access, data storage and retrieval, web hosting, virtual private networks, intranets, telephone systems, and cable face new responsibilities and obligations under the PATRIOT Act. Issues that fall under this area include:

- Authority to Intercept Voice Communications in Computer Hacking Investigations Section 202 of the PATRIOT Act amends the Computer Fraud and Abuse Act (18 U.S.C. § 2516(1) and permits the use of pen register and trap and trace devices, previously limited to recording the numbers dialed on a telephone line, to trace the "dialing, routing, addressing, and signaling information" of electronic communications (e.g., phone or other communications device).
- Obtaining Voice-mail and Other Stored Voice Communications - Section 209 of the PATRIOT Act alters the way in which the wiretap statute and Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 apply to stored voice communications. The amendment allows for nationwide orders for pen/trap devices and search warrants for e-mail issued by a judge but that apply outside of the issuing district. This means that a wiretap order targeted to a particular person is no longer confined to a particular computer or telephone. Instead, the wiretap may rove wherever the target goes. Additionally the amendment ensures that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications (e.g. voice mail) using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

- Scope of Subpoenas for Electronic Evidence Section 210 of the PATRIOT Act amends the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 (c) to expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The unamended section 2703 allowed law enforcement to obtain a limited class of information including customer's name, address, length of service, and means of payment. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the Internet Service Provider (i.e., ISP) to the customer/subscriber for a particular session, as well as the remote IP address from which a customer connects to the ISP. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

The amendment also clarifies that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for their account with communications provider, "including any credit card or bank account number." While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users biographical information.

- The broadened use of subpoenas requiring the disclosure of user records "relevant" to an investigation, a lower standard than the previous need for "probable cause". Section 215 amends the Foreign Intelligence Surveillance Act (FISA) to allow the FBI to obtain a court order for any tangible things, without probable cause from a secret court.

Any tangible things include books, record, papers, documents, and other items for an authorized investigation to protect against terrorism or clandestine intelligence activities. Thus, any tangible thing" can include a record of what books have been checked out from a library and Internet use records.

Section 215 also forbids persons producing such "tangible things from disclosing to anyone that the FBI requested such information.

- Subpoenas for business records under FISA that override library confidentiality laws.
- Immunity for compliance with FISA wiretap (Section 225) in accordance with a court order or request for emergency assistance as detailed in the PATRIOT Act.
- The section on computer trespass (i.e., Section 217) by unauthorized users that include violations by hackers. Section 217 allows (but does not require) an ISP to enlist the help of law enforcement when it discovers a hacker/computer trespasser. Note that a computer trespasser does not include a person known by the owner or

operator. This statute cannot be used against an ISP's own users. This section also protects the government from liability if it conducts warrantless wiretaps of computer trespasses.

- The requirement for Immigration and Naturalization Service to develop a database (i.e., SEVIS) for processing and tracking all foreign students and visitors beginning on January 1, 2003.

Sixteen provisions of the Patriot Act were originally scheduled to sunset on December 31, 2005 however, after the law was extended twice, legislation was passed in March 2006 which reauthorized these provisions. Three provisions of the renewed act will be reviewed in four years; the other provisions are permanent. The Act was also amended with new protections to the 2001 antiterrorism law being added in three areas. The renewed Act:

- Gives recipients of court-approved subpoenas for information in terrorist investigations the right to challenge a requirement that they refrain from telling anyone.
- Eliminates a requirement that an individual provide the FBI with the name of lawyers consulted about National Security Letters, which are demands for records issued by investigators.
- Clarifies that most libraries are not subject to demands in those letters for information about suspected terrorists.

The PATRIOT Act also amends sections of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703 et seq., and the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to aid in the deterrence and prevention of cyberterrorism (e.g., development of cybersecurity forensic capabilities, amendment of sentencing guidelines relating to certain computer fraud and abuse, etc.).

The civil (financial) and criminal penalties for violations of the PATRIOT Act can be severe. Criminal penalties such as fines or imprisonment may apply. It is therefore imperative that the University, its legal counsel and its staff be informed about these changes and properly trained so that they can comply with proper search warrants, subpoenas and wiretap requests from law enforcement under provisions of the act.