A Cyberspace Law Update – Part I: Student Issues

Rodney J. Petersen

Director, Policy and Planning

Office of Information Technology

University of Maryland

23rd Annual National Conference on Law and Higher Education
Clearwater Beach, Florida
February 17-19, 2002

Pamela is a Pirate

Pamela uses a peer-to-peer file sharing application for swapping her mp3 music files with others on the network. The high speed internet connection in her residence hall room provides a static IP address that facilitates the sharing of music and video files. A network administrator notes a spike in the outgoing bandwidth use from Susie's network connection and discovers the transfer of large data files with the file name HarryPotter.mov

- What should the network administrator do?
- What policies and procedures should be in place?
- Is there a role for policy enforcement and education?

Appropriate Policy Interventions

- Acceptable Use and Peer-to-Peer Technology
- Bandwidth Management
- Copyright Infringement Procedures
  - DMCA Agent and Web Site Notice
  - Policy That Provides for Termination of Account of Repeat Infringers
  - “Notice and Take Down” Procedure
  - Informational Materials that Promote Compliance with U.S. Copyright Laws

Terry is a Terrorist

Terry, a student with suspected terrorist connections, is the subject of ongoing law enforcement monitoring and surveillance. The FBI approaches the administrator of the institution's email system to request her cooperation in accessing all of the student's stored and future electronic communications.

- What information is the system administrator likely able to provide?
- What will the FBI be required to produce?
- What should institutions do to prepare for increased electronic surveillance?

Appropriate Policy Interventions

- Acceptable Use and Privacy Expectations
- Electronic Surveillance
- Collection and Disclosure of Personal Information
- Directory Services and User Accounts
- Logging and Monitoring Practices
- Protocols for Responding to Requests

Privacy Expectations

- University of Maryland Guidelines for the Acceptable Use of Computing Resources – http://www.umd.edu/aug

Electronic Surveillance

- **Interception orders** authorizing the interception of communications
- **Search warrants** authorizing the search of physical premises and seizure of tangible things like books or other evidence
- **"Pen register" and "trap-and-trace device" orders** (pen/trap orders), which authorize the collection of telephone numbers dialed to and from a particular communications device; and
- **Subpoenas** compelling the production of tangible things, including records.

Harry is a Hacker

Harry gains unauthorized access to your computer system by compromising an account of one of your students. He unsuccessfully attempts to login to your student information system and human resources system. He successfully uses his access to cause a distributed denial of service attack on a small Internet Service Provider in another State.

- What does the computer system administrator do upon learning of this intrusion?
- How do you respond to the threat of lawsuit from the affected ISP?
- How do you prevent unauthorized access in the first place?

Appropriate Policy Interventions

- Acceptable Use and Unauthorized Access
- Computer and Network Security
  - IT Security Plan
  - IT Security Policy and Guidelines
  - Vulnerability Testing and Intrusion Detection
  - Incident Response Protocol
- Investigating Computer Trespassers
  - USA PATRIOT Act and Computer Crimes Statutes
  - Login Banners

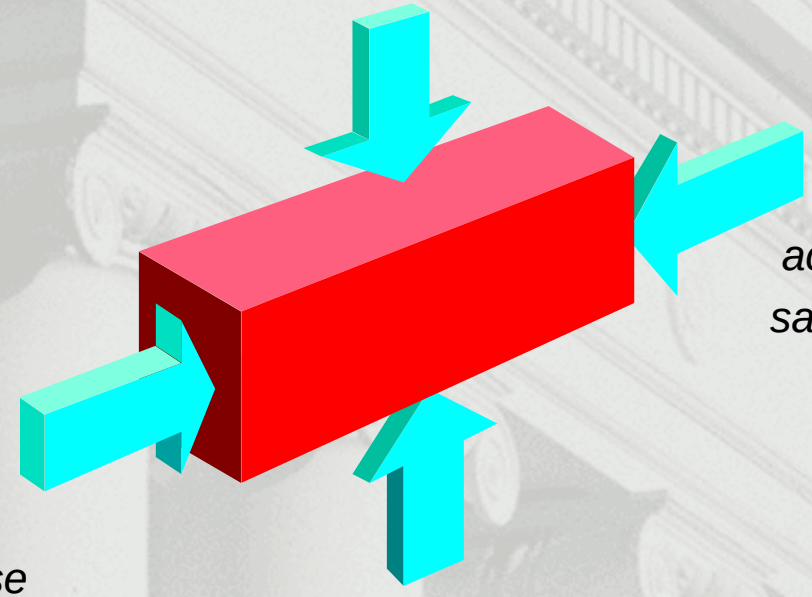
Login Banners

NOTICE: Unauthorized access to this computer is in violation of Article 27, Sections 45A and 146 of the Annotated Code of Maryland. The University ***may*** monitor use of this system as permitted by State and federal law, including the Electronic Communications Privacy Act, 18 U.S.C. sections 2510 et seq. Anyone using this system acknowledges that all use is subject to University of Maryland Acceptable Use Guidelines available at www.umd.edu/aug

Policy Framework

Law

Constitution, federal & state laws, liability



Values

academic freedom

safety and security

privacy

Ethics

netiquette

appropriate use

Morality

pornography & indecency

Federal and State Law

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)
- Foreign Intelligence Surveillance Act (FISA)
- Electronic Communications Privacy Act (ECPA)
- Family Educational Rights and Privacy Act (FERPA)
- Computer Fraud and Abuse Act (CFAA)
- State Computer Crimes and Wiretap Laws

Competing Values

Crime Control vs. Due Process

Surveillance vs. Privacy

Monitoring vs. Secrecy

Safety vs. Danger

Restrictions vs. Mobility

Security vs. Open Systems

Accountability vs. Autonomy

Consequences vs. Free Will

Privileges vs. Rights

Rights vs. Responsibilities

Rights and Responsibilities

- Rights
  - Due Process
  - Reasonable Expectations of Privacy
  - Safety and Security
  - Confidentiality and Need to Know
  - Freedom of Speech
- Responsibilities
  - Obey the Law
  - Follow Institutional Policies and Procedures
  - Respect the Rights of Others
  - Treat Others Fairly
  - Promote Ethical Behavior

Next Generation of Acceptable Use

1. End-User Agreements
   - Terms and Conditions of Use
   - Service Level Agreements
2. Modification of Existing Policies
   - Harassment and Discrimination
   - Intellectual Property
3. Technology Specific Guidelines
   - Electronic Mail and Internet Use
   - Web Site Development and Operations
4. Policies Resulting From Legal Requirements
   - Privacy and Data Security
   - Accessibility of Information Technology