A Cyberspace Law Update – Part II: Academic 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

Copyright Law Developments

- Distance Education – Introduction of TEACH Act
- Authors Rights
  - New York Times v. Tasini
- Section 1201 Anti-Circumvention Clauses
  - Rulemaking by U.S. Copyright Office
  - Felten v. RIAA and Universal City Studios v. Riemierdes
- Copyright Term Extension
  - Eldred v. Ashcroft and Golan v. Ashcroft
- Section 104 Study and “First Sale” Doctrine
- Database Legislation

UCITA Update and Implications

- Uniform Computer Information Transactions Act
  - Uniform – unify contract law of 50 states and replace uniformity of federal copyright law
  - Computer Information – information in electronic form: copyrighted materials plus
  - Transactions Act – negotiated contracts and mass market (“shrinkwrap” and “click-through”) license agreements
- Passed in 2000 by Maryland in Virginia
- Controversial, Complex, and Catastrophic!

Intellectual Property Policies

- Copyright Issues
  - Ownership of Courses, Software, & Scholarly Publications
  - Use of Copyrighted Materials
- Trademark Issues
  - Protection of University Trademarks, Domain Name Controversies, and Use of University Name
- Patent Issues
  - Technology Transfer and Commercialization of Research
- Related Policies
  - Conflict of Interest and Commitment
  - Consulting and Use of Institutional Resources

“Safe Computing Environment”

- Proposal to amend OMB Circular A-110 (Uniform Administrative Requirements for Grants and Agreements With Institutions of Higher Education), based on the “drug-free workplace” requirements to create a “safe computing environment”
- Purpose: To clarify procedures by which grantees may adequately safeguard IT assets acquired or otherwise funded under the grant and assure those assets are used solely for authorized purposes as required by OMB Circular A-110.

Proposed Security Requirements

- A grantee, other than an individual, shall certify to the agency that it will provide a safe computing environment;
- A grantee who is an individual shall certify to the agency that, as a condition of the grant, he or she will maintain support IT assets in a safe manner ensuring it is used only for authorized purposes.

Proposed Elements of Certification

Publication of a statement notifying employees that

(1) unauthorized use of computing resources is prohibited and listing unauthorized uses of computing resources, and

(2) when an IT system is used to attack other users for purpose of harassment, unauthorized access, and/or denial of service, through a network, the system may be removed from the network immediately and may remain disconnected until the conditions leading to its use in such attacks have been eliminated, and

(3) any significant security event must be reported within three calendar days of its discovery, specifying the actions that will be taken against employees for violation of such prohibition.

Proposed Elements (cont'd)

- Each employee engaged in the performance of the grant must be given a copy of the above statement
- Statement will notify employee that, as a condition of employment under the grant, the employee will abide by the terms of the statement
- Take one of the following actions, within a reasonable time after learning of a significant computer security event that puts other systems on the network at risk:
  (1) Remove the system from the network or
  (2) Place a firewall between the system and the network that adequately protects other systems on the network

Implications for Higher Education

- "Safe Computing Environment" is *just* a proposal!
- Heightened concern about college and university computer networks is a reality!
- Security requirements from federal, state, and other entities are coming (if not already here)!
- There is a huge gap in awareness among higher education executives about the extent of the problem and potential risks!
- Extent and types of liability is unknown but certain!
- "Best Practices" probably already exist and need to be identified, evaluated, and promoted!

“Middleware” and Enabling Technologies and Services

- Middleware: a layer of software between the network and the applications. It includes a set of services designed to provide a framework for network based applications to do enterprise based authentication, authorization, and security.
- Directory Services: contains certain information about the members of the university community (faculty, staff, students, alumni, and affiliates”) that may be used for authentication, authorization, and security.

Trust in Electronic Communications

- **Authentication** – process used to reliably identify the person or entity
- **Authorization** – verification that a person has the legitimate authority to perform the requested activities
- **Data Integrity** – assurance that the content has not been altered or compromised
- **Confidentiality** – ensures that only the intended audience can read the communication
- **Nonrepudiation** – the legal, ethical, and technical assurance of a signed document and enforceability of a communication

Public Key Infrastructure (PKI)

PKI is a collection of technical services, policies, and business practices that can support the five critical aspects of trust (authentication, authorization, data integrity, confidentiality, and nonrepudiation) across network communications.

Practical and Policy Issues

- Digital Certificates
- Certificate Authorities
- Certificate Policies
- Federal Bridge Certification Authority (FBCA)
- Higher Education Bridge Certification Authority (HEBCA)

Implications for Higher Education

- PKI technology is evolving and not ubiquitous
- Distance education and other inter-institutional collaborations and resource sharing arrangements will require new policy and technology solutions
- The legal, policy, and technical issues are complex and will require the help and participation of multiple constituencies
- EDUCAUSE, representing the IT leadership of higher education, will form a policy board with de facto authority to support the implementation of a Higher Education Bridge Certificate Authority

PKI Resources

- **PKI for Networked Higher Education**
  http://www.educause.edu/netatedu/groups/pki/
- **Higher Education PKI Policy Activities Group**
  http://www.educause.edu/HEPKI/
- **Certificate Policies**
  http://middleware.internet2.edu/certpolicies/
- **American Bar Association Information Security Committee PKI Assessment Guidelines Public Draft for Comments**
  http://www.abanet.org/scitech/ec/isc/pag/pag.html
- **PKI Resources**
  http://www.educause.edu/netatedu/groups/pki/resources.html
- **Middleware Resources**
  http://www.internet2.edu/middleware/