

IT Security for Higher Education: *A Legal Perspective*

***Prepared for the
EDUCAUSE/Internet2 Computer and Network Security Task Force***



Funded by a grant from the National Science Foundation



**Kenneth D. Salomon
Peter C. Cassat
Briana E. Thibeau**

Dow, Lohnes & Albertson, PLLC

March 20, 2003

©2003 EDUCAUSE/Internet2 Computer and Network Security Task Force. This work may be reproduced and redistributed, in whole or in part, without alteration and without prior written permission, provided all copies contain the following statement: "© 2003 EDUCAUSE/Internet2 Computer and Network Security Task Force. This work is reproduced and distributed with the permission of the Security Task Force."

I. Introduction

Federal and state laws relating to privacy and information technology security have become increasingly complex in nature, and the practical effect of these laws on colleges and universities is just beginning to unfold. Recent incidents relating to information security have brought these issues to the forefront and have highlighted the liabilities that can arise when security measures are compromised. In one story that made national headlines in 2002, Yale University discovered that a member of Princeton University's admissions staff used the birth dates and Social Security numbers of Princeton applicants who had also applied to Yale to gain access to a Yale web site set up for prospective students.¹ The Princeton administrator stated that he was testing network security procedures and was not trying to gain an advantage in recruiting the students. Yale filed a complaint with the Federal Bureau of Investigation (FBI), and Princeton launched an independent investigation. In another incident, the University of Texas at Austin acknowledged that the names, e-mail addresses and Social Security numbers of some 59,000 students, alumni and employees were obtained through a brute force attack on a University database. According to the University, the incident could have been prevented if additional security measures were taken.²

The University of Kansas also found itself in the media spotlight when it discovered that the computers in its international students office had been hacked on at least five occasions and personal information on more than 1,400 foreign students had been stolen.³ The information included Social Security numbers, dates of birth, passport numbers, phone numbers and countries of birth. The University had collected the information for the Student and Exchange Visitor Information System (SEVIS), a database that is being developed by the Immigration and Naturalization Service (INS) to monitor and track foreign students. The INS is under a mandate to create the database pursuant to the USA PATRIOT Act, and colleges and universities that enroll international students must participate in the system or forfeit their right to enroll those students. University officials report that the temporary "hole" in their security system has been closed. However, this incident has prompted the FBI to investigate possible connections to terrorism, and has prompted affected students to worry about identity

¹ See Karen W. Arenson, *Princeton Pries Into Web Site for Yale Applicants*, the New York Times, July 26, 2002, available at <http://www.nytimes.com/2002/07/26/education/26IVY.html>; Diane Scarponi, *Yale Accuses Princeton of Hacking*, the Washington Post, July 25, 2002, available at <http://www.washingtonpost.com/ac2/wp-dyn/A2411-2002Jul25>; Michael Barbaro, *Princeton Apologizes for Web Breach*, the Washington Post, July 30, 2002, available at <http://www.washingtonpost.com/ac2/wp-dyn/A18705-2002Jul29>.

² See Ralph K. M. Haurwitz, *Hackers steal vital data about UT students, staff*, Austin American-Statesman, March 6, 2003, available at www.austin360.com/aas/metro/030603/0306uthack.html.

³ See Michael Arnone, *Hacker Steals Personal Data on Foreign Students at U. of Kansas*, the Chronicle of Higher Education, Jan. 24, 2003, available at <http://chronicle.com/free/2003/01/2003012403n.htm>; Julie Mah, *Foreign-student database at KU hacked*, The Wichita Eagle, Jan. 24, 2003, available at www.kansas.com/mlid/kansas/5019148.htm.

theft and the possibility of facing additional questions at U.S. ports of entry when entering or leaving the country. Recognizing the risk posed to its students, the University is trying to contact every student affected by the security compromise.

Each incident illustrates the unforeseen risks that can be associated with information technology assets. For educational institutions, the importance of such assets continues to grow as the 21st Century institution is both increasingly computerized and increasingly networked. Everything from transcripts to course syllabi to student financial aid records are stored in databases on servers that without the use of appropriate safeguards to restrict against dissemination can be accessed from both within and outside the institution. Office hours are some times replaced by e-mail, and virtually every institution claims to offer at least some form of online learning. The increasing digitization and dissemination of content for online use and the sprawling growth and interconnectivity of campus networks have allowed professors, students, and other members of the educational community to exchange ideas and information in ways only imagined a few years ago. But this proliferation of access and interconnectivity brings with it increasing risks. Unlike private corporate networks, which, by their nature, are designed to be “walled gardens” of information, campus networks – due to the need to facilitate collaboration and provide access to information – generally are designed to be more open, and therefore more vulnerable to misuse.

Not only can an educational institution’s computer systems be the target of unauthorized access from outside the institution, but individuals with access to those powerful systems can use them to launch unauthorized attacks on other computer systems and networks. Public access terminals located in college and university libraries, now a nearly universal phenomenon, are particularly vulnerable, both as a means to obtain access to institutional networks and to harass others anonymously. As a result of these trends, college and university administrators, IT professionals, and legal counsel should become familiar with the federal and state computer theft and privacy laws that may give rise to criminal prosecution or civil claims *against the institution* as well as its personnel and students.

Federal laws such as the Electronic Communications Privacy Act (ECPA),⁴ the Computer Fraud and Abuse Act (CFAA),⁵ and the Family Educational Rights and Privacy Act (FERPA),⁶ as well as state computer crime laws and common law or statutory rights of privacy may be implicated in situations where improper access is gained to a supposedly secure computer system. In many ways, however, these laws have failed to keep pace with technological innovations. The result has been an atmosphere of uncertainty, placing further strain on already scarce institutional resources and leading in some cases to inaction as a result of concerns over legal exposure. The absence of a single set of standards further complicates the issue,

⁴ 18 U.S.C. § 2701 *et seq.*

⁵ 18 U.S.C. § 1030.

⁶ 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

leaving administrators and IT directors struggling to decide how best to protect their institutions while at the same time not interfering with their educational mission.

This white paper explores the current legal landscape and the factors contributing to this atmosphere of uncertainty. The following sections present an overview of existing federal and state privacy and security related laws affecting institutions of higher education. The paper then discusses several practical implications of such laws for institutions of higher education and suggests areas for further exploration.

II. The Current Legal Landscape

The legal atmosphere in which institutions of higher education operate reflects an overlapping system of state and federal regulation. Various institutional activities may be governed by a combination of federal and state regulations, as well as by accrediting organization standards. In addition to these promulgated standards, in many cases institutions remain subject to suits based on common law negligence theories. In fact, as distance education and information technology have enabled colleges and universities to spread their reaches even farther, institutions may be subject to suit in multiple states and even foreign jurisdictions.

The likelihood that multiple federal, state and foreign laws could apply is even greater when it comes to laws that relate to the use or misuse of information technology. While there is an increased likelihood that an institution could be faced with a suit brought in another jurisdiction, it also may provide the institution with the ability to bring claims locally against defendants that hack into its systems from other states. In fact, a federal district court recently ruled that the act by an out-of-state defendant of accessing a plaintiff's servers without authorization formed a sufficient basis for the exercise of personal jurisdiction over the defendant.⁷

Federal Law

There is no single, comprehensive set of federal laws mandating either specific privacy practices or information security measures of colleges and universities.⁸

⁷ See *D.C. Micro Development Inc. v. Lange*, Civil Action No. 3:02-CV-225(H) (W.D. Ky. Jan. 28, 2003).

⁸ While the Federal Trade Commission (FTC) has aggressively pursued misleading customer data and privacy practices under its broad deceptive practices jurisdiction under Section 5 of the FTC Act, the FTC's Section 5 jurisdiction does not extend to the activities of non-profit organizations. As a result, while this white paper addresses the FTC's rules implementing the Gramm-Leach-Bliley Act, it does not address the FTC's deceptive practices enforcement initiatives. Interestingly, however, in 2002 the FTC settled two high-profile investigations into the cyber security and privacy practices of Microsoft and Eli Lilly. The consent orders in these cases may provide an indication of the security standards to which institutions can expect to be held. According to FTC Chairman, Timothy J. Muris, "When we issued those orders, we hoped and expected the business community would pay attention."

Instead, depending on the particular institution and the nature of the activity at issue, institutions may be required to comply with any number of potentially applicable federal laws and regulations. The list of relevant acronyms is daunting: FERPA, HIPAA, ECPA, and CFAA are just a few of the federal laws that include obligations applicable to educational institutions. Both the hastily-enacted USA PATRIOT Act and the recent TEACH Act also have electronic privacy and security implications. Navigating this maze of federal privacy statutes is made even more difficult due to the fact that many of the laws overlap or apply differently to different institutional activities.⁹

1. Family Education Rights and Privacy Act (FERPA)

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing “personally identifiable education information,” such as grades or financial aid information, without the student’s written permission.¹⁰ FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action,¹¹ the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law.¹²

One of the most significant, current risks under FERPA is that the number of electronic records created by or relating to students that are stored in college and university databases on servers has increased exponentially, increasing in turn the number of potential “educational records” that must be protected. Faculty want the

⁹ It also is noteworthy that the current Congress, like Congresses past, is considering additional privacy-related laws that, if passed, will only add to the complexity in this area. Some, such as the Online Privacy Protection Act of 2003 (H.R. 69), are quite broad, while others address more specific privacy concerns. See, e.g., H.R. 70 (proposing restrictions on the use of Social Security numbers (SSNs) by Internet Service Providers (ISPs)); H.R. 71 (proposing restrictions on the use of wireless call location information); H.R. 637 (proposing to limit the use of SSNs and impose criminal penalties for misuse); S. 153 (proposing criminal penalties for “aggravated identity theft”).

¹⁰ 20 U.S.C. § 1232g(b).

¹¹ See *Gonzaga University v. Doe*, 122 S. Ct. 2268 (June 20, 2002) (holding that an individual does not have the right to sue a school on the basis of an alleged violation of FERPA).

¹² In *Gonzaga University v. Doe*, the Supreme Court clarified that FERPA's nondisclosure provisions have an “aggregate” focus and are not concerned with whether the needs of any particular person have been satisfied. See 122 S. Ct. 2268, 2278 (June 20, 2002). Therefore, a school can avoid losing its funding by “substantially complying” (i.e., making it a custom to comply) with FERPA, and a single FERPA violation would not be grounds for denying federal funding. See *id.*; see also *Appelberg v. DeVilbiss*, No. Civ. A00-0202-BH-C (S.D. Ala. Jan. 30, 2001) (stating that an isolated incident is not enough to amount to a custom and concluding that there was no evidentiary basis for plaintiffs' contention that a custom or practice existed of releasing information from student records at the defendant school without the student's consent in violation of FERPA).

convenience of submitting grades electronically; students want to retrieve grades and register for courses via a web-enabled student information system; financial aid offices want to electronically process applications for loans and grants. In addition, course materials are increasingly transmitted and stored electronically. Deciding what constitutes an educational record subject to FERPA, therefore, is increasingly complex in the current technological environment. This ambiguity, combined with the proliferation of electronic records and the need to protect against unauthorized disclosure, threatens to significantly increase the costs and risks of exposure for security breaches.

There also is an absence of precedent regarding whether FERPA should be interpreted to apply to disclosures of student records occasioned by unauthorized access to an institution's network or databases. This issue was touched upon in a 2001 court decision which declined to impose liability based upon the "defendants' alleged 'policy of inaction by failing to implement safeguards to prevent unauthorized disclosure of educational records'"¹³ According to the court, ". . . the defendants [we]re entitled to immunity inasmuch as no precedent ha[d] ever held similar defendants liable for such conduct or inaction."¹⁴ Thus, while an argument can be made that FERPA only should apply to affirmative disclosures of educational records, and while the courts have not yet dealt with this issue head-on, it is possible that FERPA could be read to impose liability where the steps taken by the institution fail to adequately protect against unauthorized access by third parties.

An institution may be particularly vulnerable to a FERPA violation if it can be shown that it was negligent in instituting procedures to protect against disclosure of electronic records. At the same time, however, continuous changes in the technology environment, combined with the often decentralized nature of institutions' networks, make it difficult to ensure that appropriate practices are in place. For example, the movement away from mainframe systems and toward distributed databases and servers has made it more difficult to have consistent and clear data access policies and procedures. It also is uncertain under what circumstances it is necessary to use technological measures to maintain the confidentiality of educational records. While institutions appear to be moving toward securing e-mail and electronically stored records through encryption, there is no consensus as to when it is necessary to protect data or the methods that should be employed.

¹³ See *Appelberg v. DeVilbiss*, No. Civ. A00-0202-BH-C (S.D. Ala. Jan. 30, 2001) (involving unauthorized access by a school secretary's daughter to the physical – *i.e.* non-electronic – records of the plaintiff's son).

¹⁴ See *id.* at *4, n.5 (S.D. Ala. Jan. 30, 2001). The court stated that the plaintiffs presented "no legal authority, and none exists, which earlier defined, or even now defines, a 'release' under FERPA to mean the mere unauthorized access of a student's records by a fellow student without the knowledge of the school superintendent, principal or any other staff member or faculty member." See *id.* at *4. The court went on to say that "[n]o other case has ever, in factual terms, staked out a bright line establishing that the mere unauthorized access to student records, whether or not resulting from some failure on the part of the defendants to provide a security system within some previously defined parameters which prevents such access, would constitute a violation of FERPA." See *id.*

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was enacted to protect the rights of patients and participants in certain health plans. In 2000, the federal Department of Health and Human Services adopted copious regulations granting consumers the right to receive written notice of the information practices of entities subject to HIPAA. Colleges and universities that are affiliated with health care providers are considered covered entities and by April 14, 2003, those institutions must provide written notice of their affiliated health care provider's electronic information practices. Most employer-sponsored health plans also are considered to be "entities" subject HIPAA. As a result, various compliance obligations are imposed on colleges and universities that sponsor and administer such plans. The deadline for health plan compliance also is April 14, 2003 (except that health plans with annual receipts of \$5 million or less have until April 14, 2004 to comply).¹⁵

HIPAA generally requires covered entities to (i) adopt written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed; (ii) require their business associates to protect the privacy of health information; (iii) train their employees in their privacy policies and procedures; (iv) take steps to protect against unauthorized disclosure of personal health records; and (v) designate an individual to be responsible for ensuring the procedures are followed.¹⁶ Educational institutions may be obligated to comply with HIPAA in connection with a broad range of activities. College and university attorneys and their clients have been forced to dedicate significant resources in attempting to comply with the complex language of HIPAA and in applying it to the distributed environment of a typical campus, particularly as to how its enforcement coincides with other institutional obligations.

3. Electronic Communications Privacy Act (ECPA)

Unlike FERPA and HIPAA, which are specific to certain types of entities, the ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication.¹⁷ Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications.¹⁸ In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved.¹⁹ As a result, the monitoring

¹⁵ See Gerald W. Woods, *HIPAA Privacy Rule Primer for the College or University Administrator*, prepared for the American Council on Education, December 2002, available at <http://www.acenet.edu/washington/policyanalysis/HIPAA.2.pdf>.

¹⁶ Pub. L. No. 104-191 (1996).

¹⁷ See 18 U.S.C. § 2511.

¹⁸ See *id.* at § 2510(8).

¹⁹ See *id.*

by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA.

The ECPA also prohibits unauthorized access to or disclosure of electronically stored wire and electronic communications.²⁰ More specifically, the ECPA imposes liability on any person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or exceeds an authorization to access that facility, if that person thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage.²¹ While the ECPA restricts providers of *public* electronic communication services (specifically, providers of public access terminals and other public services) from divulging the contents of stored electronic communications, it does not appear to place the same restrictions on providers of *private* electronic communication services. Institutional e-mail systems and networks most likely would constitute private electronic communication services that enjoy the relaxed restrictions of the latter category, thus allowing institutions to monitor and access student e-mail accounts. Nevertheless, college and university computer use policies often strike a balance between student privacy rights and network security concerns by authorizing inspection by the institution of student e-mails or other communications *only* when there is reasonable basis to suspect improper use of a computer or network. In addition, educational institutions' networks often serve multiple communities of users (for example, students, faculty, employees, alumni, and the general public) and the correct application of the ECPA may depend on the nature of the relationship between the institution and the user. Thus, an institution's right to monitor electronic communications, or its obligation or ability to comply with a law enforcement request, may vary depending on whether the user in question is a student, an employee, or a member of the public.

The ECPA also contains specific exceptions allowing disclosures to law enforcement agencies under certain circumstances. Certain provisions of the USA PATRIOT Act, discussed below, substantially broaden the authority of law enforcement officials to obtain information under the ECPA. Under Section 210 of the USA PATRIOT Act, the scope of information that the government can obtain by subpoena has been expanded to include electronic communications, and law enforcement officials now can obtain information such as means and sources of payment, records of session times and duration, length of service and type(s) of service utilized, and user number or identity, including any temporarily assigned network addresses. Also, Section 212 of the USA PATRIOT Act amended the ECPA to permit communications service providers to release both content and non-content information about a wire or electronic communication to a law enforcement agency if the provider reasonably believes that the information must be provided without delay to avoid injury to any person. This provision of the ECPA was further amended, however, by the Cyber Security Enhancement Act of 2002, and it now permits communications service providers to divulge to a Federal, State, or local governmental entity the contents of a communication if the provider

²⁰ See 18 U.S.C. §§ 2510 – 2521, 2701 *et seq.*

²¹ *Id.*

believes in “good faith” that “an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.”²² In other words, in responding to an emergency situation, institutions are now allowed to release relevant information, including not just the existence but also the *content* of wire and electronic communications, to law enforcement officials if the institution in good faith determines that release of the information is necessary to avoid injury.

These changes have significance for institutions that essentially function in the role of Internet service provider, and the result has been to make it more complex and burdensome to respond appropriately to requests for information from law enforcement agencies. Service providers most likely can expect that, because the government now has easier access to warrants and other authority to intercept communications of all kinds, new demands will be placed on their systems and their information processing and retrieval capability.

The ECPA’s reach is long: a University of Delaware student who in the summer of 2002 obtained unauthorized access to the University’s computer system to give herself passing grades in three spring semester courses potentially violated the ECPA. In that case, the student allegedly called the University’s human resources office and impersonated her instructors to obtain new passwords, which in turn enabled her to log into the system as though she were her own professors.²³ No federal charges were brought under the ECPA, but the student pleaded guilty to misdemeanor charges on counts of criminal impersonation, unauthorized access to a computer system, and misuse of computer system information. She was sentenced to three years probation and ordered to pay \$12,000 in restitution. Three counts of felony identity theft were dropped. The University, meanwhile, began reviewing its computer security measures and charged the student with three counts of academic dishonesty and three counts of violating the school’s “responsible computing” code.

4. Computer Fraud and Abuse Act (CFAA)

The CFAA criminalizes unauthorized access to a “protected computer” with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer.²⁴ A “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States.²⁵ In light of the “interstate or foreign commerce”

²² See Homeland Security Act of 2002, H.R. 5005, 107th Congr. § 225 (2002). The Cyber Security Enhancement Act was approved by the House of Representatives as a stand-alone bill in July of 2002 but was incorporated into the Homeland Security Act (at § 225) just before the Homeland Security Act’s passage.

²³ See Brock Read, *U. of Delaware Student Is Charged With Breaking Into Computer System and Changing Her Grades*, the Chronicle of Higher Education, July 17, 2002.

²⁴ 18 U.S.C. § 1030(a).

²⁵ *Id.* at § 1030(e)(2).

criterion, the act of “hacking” into a secure web site from an out-of-state computer, which may have occurred when the Princeton admissions officer accessed Yale’s “secure” web site, could be considered a CFAA violation (although both schools took pains to say that they were not seeking any civil or criminal prosecutions). The fact that both ECPA and CFAA are *criminal* statutes considerably raises the ante.

5. USA PATRIOT Act

The USA PATRIOT Act,²⁶ passed six weeks after September 11, 2001, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA),²⁷ in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can seize with a court order certain business records pursuant to an investigation of “international terrorism or other clandestine intelligence activities,” and record-keepers are prohibited from disclosing the FBI’s action to anyone “other than those persons necessary to produce the tangible [records]” The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources – thus, librarians may not even reveal that an inquiry has been made.

The USA PATRIOT Act also amends the portion of the National Education Statistics Act of 1994 (NESA)²⁸ that specified that data collected by the National Center for Education Statistics (NCES) may only be used for statistical purposes. The amended NESA now permits the attorney general to petition a judge for an *ex parte* order requiring the Secretary of the Department of Education to provide data from the NCES that are identified as relevant to an authorized investigation or prosecution concerning national or international terrorism. In other words, data collected by NCES may now be used with a judge's order for matters relevant to an offense concerning terrorism. Nonetheless, the attorney general is obligated to protect the confidentiality of any NCES data it obtains.²⁹

²⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, H.R. 3162, Title II Section 215 (Oct. 26, 2001).

²⁷ Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-62).

²⁸ 20 U.S.C. § 9007, *et seq.*

²⁹ Following the enactment of the USA PATRIOT Act, the 107th Congress enacted the E-Government Act of 2002, H.R. 2458, 107th Congr. (2002). Sections 511 through 513 of the E-Government Act require that all individually identifiable information supplied by individuals or institutions to a federal agency for statistical purposes under the pledge of confidentiality must be kept confidential and may only be used for statistical purposes. See H.R. 2458, 107th Congr. §§ 511-513 (2002).

Another significant impact of the USA PATRIOT Act is its mandate to the INS requiring the INS to develop and implement the Student and Exchange Visitor Information System or “SEVIS.” SEVIS is an Internet-based system that will allow schools to transmit information on foreign students to the INS for purposes of tracking and monitoring. The system will compile students’ personally identifiable information including admission at port of entry, academic information, and disciplinary information. FERPA’s restrictions have been waived to allow schools to disclose this information, which must be maintained and updated for the duration of a student’s stay in the United States.

As noted in the Introduction, above, recent events at the University of Kansas illustrate that efforts to require the creation of records for national security purposes may have unintended consequences. A hacker gained access to the computers in the University of Kansas (KU) international students office and obtained the SEVIS records for approximately 1,450 international students. Ironically, the hacker apparently exploited a security “hole” created while KU officials were updating the security features on the computer that maintained these records. The information that the hacker accessed from KU included personally identifiable information which could be used, along with other materials, to create fake passports, visas, and other documentation, as well as for other forms of identity theft. This incident illustrates that the creation of SEVIS may have the unintended consequence of compromising student privacy in the interest of public safety. Speaking in January of 2003 at a regional education conference, Frank J. Cilluffo, executive director of the President’s Homeland Security Advisory Council, suggested as much when he stated that “we’d like to know if someone from a certain country changed their major from English literature to nuclear physics, or something along those lines.”³⁰

6. TEACH Act

The TEACH Act, passed by Congress on October 3, and signed into law by the president on November 2, 2002, relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use materials in technology-mediated educational settings.³¹ But the new law carries with it obligations that have privacy and security implications: institutions that want to take advantage of the relaxed copyright restrictions must limit “to the extent technologically feasible” the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information.³² In other words, the TEACH Act may require institutions to

³⁰ See Florence Olsen, *Demands of Homeland Security Will Pressure Colleges, Campus Computing Experts Warn*, the Chronicle of Higher Education, January 17, 2003, available at <http://chronicle.com/free/2003/01/2003011702t.htm>.

³¹ Technology Education and Copyright Harmonization (TEACH) Act of 2001, H.R. 2215, *codified at* 17 U.S.C. §§ 101(1), 112(f).

³² See *id.*

implement technical copy protection measures and to authenticate the identity of users of electronic course content.³³

The implementation of digital rights management tools necessary to control access will create additional cost, complexity, and yet another set of electronic records. Enforcement of the required protections also will raise new issues about appropriate disciplinary measures, not to mention the privacy concerns arising from monitoring student usage of course materials for unauthorized use or dissemination. Among other things, institutions may be confronted with claims under the Digital Millennium Copyright Act (DMCA) if their users attempt to defeat the technological restrictions employed by digital rights management tools. The DMCA makes it unlawful to circumvent technological measures that effectively control access to protected works.

7. Gramm – Leach – Bliley Act (GLBA)

The GLBA³⁴, enacted in 1999, is applicable to financial institutions, including colleges and universities, and creates obligations to protect customer financial information. The GLBA includes requirements to take steps to ensure the security of personally identifying information of financial institution customers, such as names, addresses, account and credit information, and Social Security numbers.³⁵ The GLBA also sets forth extensive privacy rules which, among other things, require covered financial institutions to provide customers with privacy statements describing their information privacy practices. However, the Federal Trade Commission's (FTC's) regulations implementing the GLBA specifically provide that colleges and universities will be deemed to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. Nevertheless, educational institutions likely remain subject to the security provisions under the GLBA and the FTC's implementing rules. The GLBA customer financial information security rules, with which institutions must come into compliance by May 23, 2003, will require colleges and universities to develop comprehensive security programs, assess the need for employee training, and include obligations in their agreements with third parties that have access to financial records covered by the rules.³⁶

³³ For guidance on the technological considerations of the TEACH Act, see *Technological Requirements of the TEACH Act*, American Library Association, EDUCAUSE and the Association for Computing Machinery (2003), available at <http://www.educause.edu/asp/doclib/abstract.asp?ID=CSD2725>.

³⁴ Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

³⁵ For guidance on the GLBA Safeguards Rule, see *Financial Institutions and Customer Data: Complying with the Safeguards Rule* (September 2002), available at <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>.

³⁶ For additional information concerning educational institutions obligations under the GLBA, see the National Association of College and University Business Officers January 13, 2003 Advisory Report, entitled *Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information*, available at http://www.nacubo.org/public_policy/advisory_reports/2003/2003-01.pdf.

State Law

Institutions naturally tend to worry most about federal requirements that constrain their actions or increase their costs. But in addition to the variety of federal laws that are applicable to information security and privacy, there are numerous state laws relating to security and privacy. Many states have enacted computer crime laws that expressly criminalize tampering with computers or accessing certain computerized records without authorization. For example, under Connecticut law, it is unlawful for any person to use a computer or computer network without authority and with the intent to remove, halt or disable computer programs or software; cause a computer to malfunction, alter or erase any computer data or software; cause physical injury to the property of another; or make an unauthorized copy of computer data or software.³⁷ Virginia and Rhode Island have enacted laws that are nearly identical to Connecticut's,³⁸ and several other states have passed similar laws.³⁹ In addition, most states recognize a right to privacy, either by statute or by common law, which broadly speaking includes the right to be free from "unwanted intrusion upon seclusion or solitude" or the "public disclosure of private affairs."

Moreover, the absence of comprehensive federal privacy standards has led to a proliferation of state information privacy laws. For example, several states are considering or have enacted privacy legislation that deals with collection of information relating to children, disclosure of health care information, or collection of consumer information. Other laws have been developed to deal with very specific privacy concerns. Many states have laws that expressly provide for the confidentiality of library records, including patron information.⁴⁰ Other states have passed laws that restrict the use and/or disclosure of Social Security numbers (SSNs).⁴¹ New York, for example, limits the use of SSNs in schools and colleges. The legislation specifically bars the display of a student's SSN in a posting or public listing of grades, on class rosters or other lists provided to teachers, on student identification cards, and in student directories or similar listings. As a result, many public and private schools in the State are opting instead to assign students identification numbers.⁴² Arizona has a similar statute that specifically restricts the use of SSNs by educational institutions. The

³⁷ Conn. Stat. Title 53, Chapter 949g, § 53-451(b).

³⁸ Va. Code § 18.2-152.4; R.I. Gen Laws § 11-52-4.1.

³⁹ See, e.g., Ala. Code § 13A-8-10; Cal. Penal Code § 502; Del. Crim. Code §§ 931-939; Md. Code Ann. § 146.

⁴⁰ See, e.g., Am. H.B. 389, 123d Gen. Assem., Reg. Sess. (Ohio 2000).

⁴¹ Even absent the existence of state law restrictions on SSNs, it is important to note that SSNs, in whole or in part, may constitute "personally identifiable educational information" that is protected under FERPA. See, e.g., *FERPA Advisory Letter: Disclosure of Social Security Numbers*, Family Policy Compliance Office, Dept. of Education (May 2001), available at www.nacua.org/documents/Evangelos_Gizis_Letter.pdf (advising that the use of the last four digits of student SSNs for posting grades, without prior written consent of the students, constitutes an unlawful disclosure of personally identifiable information under FERPA).

⁴² N.Y. Educ. Law § 2-b.

statute, which became effective June 30, 2002, prohibits any university under the jurisdiction of the Arizona board of regents from assigning an individual identification number to faculty, staff or students that is identical to the individual's SSN.⁴³ The statute also restricts, though does not prohibit, the use of SSNs by community colleges under the jurisdiction of the State Board of Directors for Community Colleges.⁴⁴ In California, businesses, health care providers and schools are barred from:

- Publicly posting SSNs or requiring them for access to products or services;
- Printing SSNs on cards required for accessing products or services;
- Requiring an individual to use his or her SSN to access a web site unless a password is also required to access the site; or
- Printing an individual's SSN on any materials that are mailed to the individual.⁴⁵

While many state laws fall into discrete categories, others are creating new areas of potential liability by proscribing new types of conduct or imposing new obligations. California, for example, recently enacted a law that defines the specific crime of identity theft,⁴⁶ as well as a law that requires companies that do business in California to promptly disclose to affected individuals any breach of network security that results in the disclosure of unencrypted personal information.⁴⁷ This latter requirement appears to impose an affirmative obligation on institutions to notify those parties who may have a claim as a result of their information potentially having been obtained through unauthorized access to a computer system or network. Moreover, California's municipalities also have joined in the fray by adopting local privacy ordinances regulating the disclosure of certain confidential information by financial institutions.⁴⁸

Another source of headaches for those responsible for information services at public institutions are state freedom of information (FOI) or "open records" laws. All 50 states have such laws, which generally provide citizens with access to public records. While many of these state laws model the form adopted by Congress in crafting the federal Freedom of Information Act,⁴⁹ others have developed unique FOI regulatory schemes shaped by state and local policies and special interest group intervention. Therefore, it is important for institutions and their legal advisors to remain up-to-date with the FOI decisions in their state(s). A recurring question is the definition of "public

⁴³ Ala. Code § 15-1823(A).

⁴⁴ Ala. Code § 15-1823(C).

⁴⁵ Cal. Civ. Code §§ 1798.85 – 1798.86 and 1786.6.

⁴⁶ Cal. Penal Code §§ 530.5 – 530.8.

⁴⁷ Cal. Civ. Code §§ 1798.29, 1798.82 - .84.

⁴⁸ See, e.g., Daly City Ordinance No. 1295; County of San Mateo Ordinance No. 04126; San Francisco City and County Ordinance File No. 021339.

⁴⁹ Pub. L. No. 89-487, 80 Stat. 250 (codified at 5 U.S.C. §552).

records.” Not all state FOI laws define the term, and because most of these laws were created long before networked data systems existed, it is often unclear as to whether e-mail and extra-textual electronic material, such as cookies, log files, and the like should be considered part of the “public records” required to be disclosed. This uncertainty is illustrated by a recent incident involving West Virginia University, in which Sprysoft, a software retailer, filed a FOI request with the University, asking for e-mail directory information that the University makes publicly available. Armed with the results of its request, Sprysoft sent unsolicited e-mails to each West Virginia University student offering a “WVU Academic Software Special.”⁵⁰ Aside from an interesting question regarding the use of the university name, the fact that the institution inadvertently contributed to the spamming of its students by responding to a FOI request again illustrates the complex issues and unintended consequences that can result when existing information laws are applied in a changing technological environment.

Compliance with state laws is even more challenging in the context of technology-mediated learning: an e-learning student residing in one state may be protected by a set of laws that are different from the ones that apply to the state where the institution he or she is “attending” is located, and vice versa. As a result, the student may become subject to laws very different from those of his or her home state. Where once an institution could be more content with an understanding of federal legal requirements and those of its state of domicile they are now finding it necessary to extend their knowledge base nationally and, indeed, globally. As education becomes increasingly borderless, keeping track of state laws can be an expensive proposition for institutions, and a compliance failure can bring with it the risk of criticism, reputational damage, and costly class action liability.

IV. Practical Implications: What You Can Do

✓ Analyze Applicable State Laws and Municipal Ordinances

Colleges and universities would be remiss to focus only on federal legal requirements and ignore the possibility that states or municipalities may also impose constraints in the areas of information privacy and electronic security. Many laws relating to privacy and security already are on the books at the state level, and others loom in the form of pending legislation. In addition, local governments are getting into the act, passing privacy ordinances to protect consumer rights and the confidentiality of certain types of information. With state and local laws proliferating in this area, colleges and universities would be wise to coordinate with their legal advisors to properly assess and analyze applicable state laws and municipal ordinances. Where appropriate, institutional information security specialists should work with higher education associations and their legislative liaisons to influence the legislative process.

⁵⁰ See Justin Leonard, *SEJ investigates spam mail*, the Daily Athenaeum Interactive, Nov. 21, 2002, available at <http://www.da.wvu.edu/archives/022111/news/022110,01,01.html>; David McHugh, *TECHBITS: Emotions for e-mail, university spam, Linux in China, computer chess*, Foster's/Citizen Online, Nov. 21, 2002, available at http://www4.fosters.com/tech/articles/tech_1121_02e.asp.

✓ **Assess Information Security Vulnerabilities and Risks**

The recent information security breaches highlighted above illustrate the increasingly complex challenges faced by institutions that may become subjected to computer attacks or that may face liability for the unauthorized disclosure of personal information. In the wake of these events, college and university IT administrators undoubtedly are already revisiting their network security measures and computer usage policies. At the same time, however, IT administrators should bear in mind that conducting an effective security audit is a complex process and that identifying potential weaknesses is only a part of the equation. In fact, by identifying an institution's vulnerability to unauthorized access to its electronic records, without then promptly instituting appropriate measures to remedy those vulnerabilities, the institution may only serve to heighten its potential liability should a compromise occur. A report documenting security weaknesses issued months or years before a system is compromised – and later obtained under a Freedom of Information or “open records” law request by an inquiring journalist – may in fact add to an institution's woes and result in potential liability, particularly if the weaknesses, once detected, are not remedied. The alternative is no more attractive: simply ignoring the possibility of weaknesses is no protection. Although arguably it is worse to affirmatively know of a problem and fail to act than to remain blissfully ignorant, neither is a desirable route.

✓ **Review and Update Information Security Policies & Procedures**

College and university administrators and their IT specialists should coordinate closely with each other and with their legal advisors in developing information technology and security policies. Security audits are an important component of creating and maintaining an effective security program. An institution should take care, however, to avoid simply creating a harmful paper trail, and it is important to act upon security findings within a reasonable and responsible time frame.

An institution's policies should be developed with this reaction time in mind. A good policy will be flexible enough to allow the institution to react quickly, and with some discretion, to a variety of situations. A good policy also will appropriately limit access to information based on an assessment of the threats posed to the institution's systems. In developing flexible policies, institutions will have to consider the nature and magnitude of such threats and respond with an amount of security that is commensurate with the associated vulnerability based on the sensitivity of the information that is being protected. For example, it may be sufficient to provide students access to a web site at which course materials are made available using basic password protection, while at the same time it may be advisable to deploy more stringent authentication measures in allowing root access to the institution's critical systems and information databases.

✓ **Review Personnel Policies and Procedures for Access to Sensitive Information**

Institutions should focus in particular on their policies and procedures relating to the manner in which access to sensitive information is permitted and managed. A system for effectively managing network access and retiring authorization for former students and employees can greatly improve network security. A related issue is the use of criminal background checks and their role, if any, in higher education. Background checks may be required as a condition of receiving federal contracts or grant funds, and some state laws authorize background checks for certain job positions. But such checks can become a topic of hot debate. For example, when the University of Texas (UT) announced it was adopting a new policy requiring criminal background checks of all job finalists, some faculty leaders and administrators voiced concerns that the policy would inhibit the University's ability to recruit top-notch talent.⁵¹ The outcry was so great that the University later announced that it is limiting the scope of its background check policy to only "security sensitive" positions. Three categories of positions are defined as "security sensitive" – senior-level administrators; child-care and patient-care positions; and employees with access to pharmaceuticals, select agents or controlled substances – but others can be defined as such by the various divisions of the UT system at their own discretion.⁵²

No matter how complex a scheme of background checks and security policies an institution has in place, ultimately the information security of an institution hinges on the integrity and honesty of those who are given access. This fact is well illustrated by the recent events at Texas Tech. In mid-January, it was reported that 30 vials of a deadly bacteria were missing from a Texas Tech Health Sciences Center laboratory. Only one researcher had legal access to those vials, and after only a few days of intensive FBI investigation, that prominent researcher was arrested for allegedly making false statements about the vials, which he had previously destroyed.⁵³ This story had a happy ending because the vials were not in dangerous hands, as administrators and government officials first feared. But this researcher's apparent dishonesty raises questions and concerns about the safety and security of the remaining vials. In a time when fear of bioterrorism runs high, it is not surprising that these types of issues foster considerable debate. Whether background checks, password protection, or advanced measures like biometrics are the security method of choice, institutions would be wise to develop flexible policies that will allow quick action and wide institutional discretion in their administration. It may be difficult, if not impossible, to make an institution completely secure, but an inability to act, and act quickly, in the face of security threats

⁵¹ See Linda K. Wertheimer, *Criminal checks incite UT outcry*, the Dallas Morning News, Aug. 22, 2002, available at <http://www.uh.edu/admin/media/topstories/2002/dmn/200208/20020822criminalck.html>.

⁵² See Chris Piper, *Background Checks Limited*, the Shorthorn Online, available at <http://www.theshorthorn.com/archive/2002/fall/02-dec-03/n120302-02.html>.

⁵³ See Betsy Blaney, *Missing vials of plague samples found in Texas after triggering bioterrorism fears*, Associated Press, Jan. 16, 2003, available at http://www.nlm.nih.gov/medlineplus/news/fullstory_11295.html; *Plague researcher held without bond*, Associated Press, Jan. 16, 2003, available at <http://www.msnbc.com/news/859757.asp?0cv=CB10>.

could invite reputational damage and embarrassing and potentially costly legal proceedings.

✓ **Scrutinize Relationships With Third-Party Vendors**

All institutions rely, to varying degrees, on the use of third-party vendors and service providers in order to manage their information systems, provide and maintain critical software, and furnish the telecommunications capacity that connects their networks to the Internet or other institutions or applications. It is important to realize that, as is the case with any other link in the chain, vulnerabilities resulting from the procedures and systems relied upon by these third parties can create threats to the information security of an institution's network. Institutions should keep these threats in mind when negotiating or renewing their relationships with third-party service providers. Among other things, it is important to ensure that vendors with access to the institution's confidential information are subject to obligations of confidentiality that will enable the institution to comply with its own obligations of confidentiality under relevant privacy-related laws. In addition, vendors should be contractually obligated to implement data protection and security measures that are commensurate with the sensitivity of the information they are responsible for handling or transmitting. In certain cases, such as under the GLBA, institutions may be obligated by statute to include information security obligations in their third party vendor agreements.

Educational institutions should require vendors of mission critical applications to have in place contingency plans to provide for data back-up and disaster-recovery measures necessary to allow an institution to continue functioning even in the case of a catastrophic event. It also is important to ensure that the institution's vendors are obligated – through “service level agreements” – to timely respond to and escalate problems that may compromise the integrity of the institution's operations. Lawyers for institutions of higher education also should consider including in their IT vendor agreements representations and warranties to the effect that the software and services provided by such vendors will not result in the introduction of any “harmful code,” such as Trojan horses, viruses, or backdoors. In negotiating and reviewing agreements with third-party service providers, college and university IT professionals and their lawyers also should bear in mind the potential differences among applicable state laws and seek to have their agreements governed by the laws of the state which will provide the most favorable treatment. This is particularly important in light of the recent developments in state laws described above, as well as the trend among states to enact or to consider enacting laws such as the Uniform Computer Information Transactions Act (UCITA), which to date has been adopted only in Maryland and Virginia.⁵⁴

⁵⁴ See S.B. 142 (Md. 2000); S.B. 372 (Va. 2000); see also UCITA Online, <http://www.ucitaonline.com/legalart.html>.

✓ **Review the Institution's Insurance Policies**

Educational institutions also can take proactive steps to manage their information security risks by reviewing and, where available, renewing their insurance policy coverage with an eye toward insuring against the risks of cyber security. Although the availability of cyber security coverage is a relatively new product, institutions should at a minimum review their existing insurance policies to consider the potential protections they may offer for the new types of risks they are encountering.

✓ **Develop a Rapid Response Plan and Incident Response Team**

The worst time to prepare for a response to a security failure involving the unauthorized disclosure of educational records or other personal information is after it happens. Institutions should plan ahead and have in place a plan for responding to and escalating the decision-making associated with an information security crisis. Among other things, an institution should consider designating in advance an appropriate spokesperson, incident response team, and escalation path.⁵⁵

✓ **Work Together with Higher Education Associations and Coalitions to Develop Standards Relating to Information Security**

As described above, many of the costs and potential liabilities associated with the increasingly complex challenges faced by educational institutions in the areas of information privacy and security result from the absence of uniform standards. For example, while FERPA may establish a duty on the part of educational institutions to guard against the unauthorized disclosure of educational records, there is virtually no guidance on how far an institution must go to safeguard its computer networks from unwanted intrusions. Absent such standards, institutions remain vulnerable to class action challenges in the event their information security policies and procedures fail to repel unauthorized intruders. Educational institutions at all levels would be far better served through the development and adoption of guidance in the form of recommended "best practices" or similar measures. Accordingly, institutions of higher learning should continue to work together through coalitions and the educational associations that represent them to develop sensible, national policies relating to the protection of their information assets.

FOR ADDITIONAL INFORMATION REGARDING IT SECURITY VISIT:

*The EDUCAUSE/Internet2 Computer and Network Security Task Force web site at:
<http://www.educause.edu/security>*

⁵⁵ For additional information on formulating incident response plans see Moira West-Brown, et al., *Handbook for Computer Security Incident Response Teams (CSIRTs)*, December 1998, a publication of the Carnegie-Mellon University Software Engineering Institute, available at <http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf>.