Susan Thomas

Prof. Michael Shaw

BADM 559

May 1, 2008

FERPA, Student Privacy, and Information Technology in Higher Education

Introduction

The Family Educational Rights and Privacy Act (FERPA) of 1974 requires higher education institutions to "limit the disclosure" of certain types of student information contained in education records (Hillison et al. 301). Colleges and universities trying to comply with FERPA universally have policies and procedures aimed at protecting student privacy. However, constantly changing technologies continually pose new obstacles to this protection. In this paper, I explain what FERPA is, and provide examples of FERPA violations. I also discuss the risks that information technology (IT) poses as well as the best practices and controls that higher education institutions can enact to mitigate FERPA IT risks. Finally, I explore whether FERPA goes too far (or not far enough) and the balance for colleges between protecting students' privacy while also effectively meeting students' educational needs.

FERPA Defined

FERPA is a federal law that "protects the privacy of student education records" and "applies to all schools that receive funds under an applicable program of the U.S. Department of Education" (National Center for Education Statistics 1). Failure to comply with FERPA could lead to a loss of federal funding (Hillison et al. 309). The Act gives college students four key rights: 1) the right to know what's in their education records, 2) the right to access their records,

3) the right to challenge the content of their records, and 4) the right to control access (Hillison et al. 302-303). According to Barb Wood, Assistant Registrar at the University of Illinois at Urbana-Champaign (UIUC), educational records include demographic information, admission records, grades, class schedules, printed class lists, and graded test papers. Both paper and electronic formats are covered under FERPA. There are certain items that are *not* included in the definition of an education record such as sole possession notes, campus police records, alumni records, medical records, employment records (unless contingent on being a student), and statistical data that contains no personally identifiable information about any student (Wood).

Students' rights to control access to their education records means that institutions cannot disclose information in a student's education record without the student's written consent (Hillison et al. 307). However, there are some exceptions to this rule. First, FERPA permits colleges to share information with parties that have a legitimate educational interest. These include school officials, other schools to which a student is transferring, appropriate parties connected with financial aid, accrediting organizations, government agencies with subpoenas, and more (National Center for Education Statistics 1). Institutions may also release data if they feel a health or safety emergency exists (National Center for Education Statistics 2). The important consideration for colleges is that they must make sure that a legitimate educational interest is present. For example, a student's professor cannot access a student's entire education record just because the professor works at the college. The professor can only have access to items that serve his or her educational purpose (Hillison et al. 310). In addition, parents of students in a higher education setting, including students under age 18, are not allowed access to records unless the student gives written permission, or the student is a dependent for tax purposes (Malmgren). Even if the latter applies, colleges do not have to share information with parents and have some discretion as to whether to release information to parents on a case-by-case basis. Finally, schools cannot release information for purposes of academic research, for commercial or political purposes, to random parties to conduct a mass mailing, or to student organizations. Moreover, the Freedom of Information Act (FOIA) does not allow third parties to access private student records (Wood).

Higher education institutions may disclose "directory" information without violating FERPA. Directory information could include name, address, date of birth, previous institutions attended, dates of attendance, major, class level, degrees awarded, honors, and the weight/height of an athletic team member (Wood). While FERPA provides a checklist of what items could qualify as directory information, policies vary among institutions (Orrick 90). Students also have the option to suppress directory information, but the drawback is that it could prevent the student's college from disclosing basics, such as whether a degree has been awarded. Such directory restriction could even prevent a student's name from being listed in a graduation program. At UIUC, campus employees must give the following response if asked about a student that has restricted his/her directory information: "There is no information available for any student by that name" (Wood).

FERPA permits general course information, such as syllabi and course descriptions, to be made available to the public. Class web sites may also be open for public perusal, but certain information contained in learning management systems (such as Compass) must be restricted to staff and students. This includes student photographs, online discussions, and student papers, reports, and other work (Wood).

FERPA provisions require campus employees to adequately safeguard specified data. Any documents or electronic media that contain covered data, along with personally identifiable information that would make the covered data traceable to a student or students, must be handled with caution and care (Wood).

FERPA and Privacy Violations

Higher education institutions consider possible FERPA violations as grave because of the potential loss of federal funding. However, this is not the only consequence. The release of private data has the potential to inflict serious damage to a student if his/her identity is stolen, or if negative information hinders the student’s reputation or career opportunities. In some cases, student safety could be compromised if restricted directory information (like home address) became available to a criminal. FERPA violations cause embarrassment and bad publicity for the school itself. When they occur, students and parents understandably have an outraged reaction (Jacobson 1; Dillon 1). While FERPA does not give students the right to sue (Tone and Pitts), it is possible that students could find alternative routes under which to hold institutions liable, or sue for other privacy violations not covered under FERPA. Finally, campus employees that break FERPA rules could be subject to criminal prosecution, payment of restitution, and disciplinary sanctions (Wood).

A simple Google search yields a number of privacy violations. In August 2007, an engineering professor at UIUC accidentally attached a confidential file to an email that was intended to advertise a new course. The file contained sensitive information such as name, address, grade point average, and ethnicity. The professor sent the email to 5,247 undergraduates (Jacobson 1). This incident demonstrates how easy it is for campus employees to inadvertently compromise student data. Harvard University also experienced a privacy violation when a break-in occurred to its Web server. The break-in allowed hackers to access the personal information of over 10,000 graduate housing applicants. The data included social security numbers, food allergies, and housing preferences (USA Today 3a). Ave Maria University accidentally posted private student information on its Web site, thinking it was only accessible to internal staff when it was actually accessible to the public (Dillon 1).

IT FERPA Risks

The examples in the previous section have one thing in common—they all involved computerized or electronic data. An institution's IT makes student data vulnerable in a number of ways and imposes various security risks.

Email Risks

It is common for university students to send email questions to campus officials (i.e. deans, instructors, and advisors) related to their educational records. Campus employees, in turn, often find it useful and efficient to communicate with students via email. It is also desirable for campus employees to communicate with fellow co-workers through email as well. However, email poses several dangers. First, when communicating with students, there is the risk that the person on the other end of the email is not the intended recipient. This could be due to human error such as typing an incorrect email address. It could also result from a practice called "spoofing", which Robert Morley and Clifford Rameriz define as a "fraudulent process in which someone presents an originating address in the From field that appears legitimate, even though a reply will go to another address that the person committing the fraud has supplied" (A).

Even if campus employees are sending email to the right student, a hacker could possibly gain access to the subject line or message body. Universities often opt to protect their email systems, but there is not always assurance that the student's email system does the same (Morley and Ramirez 1). The final risk with email is that campus employees may send incorrect information to the student. For instance, in the UIUC engineering example above, the sender submitted the e-mail to the correct people and was not a victim of hacking, but simply attached a file that was not intended for the entire group (Jacobson 1).

Electronic Signature Risks

FERPA allows students to "consent online to the release of transcripts and other personal data" (Foster), thereby allowing e-signatures to effectively substitute for handwritten signatures. For institutions to properly comply, students must have a secured means of providing the e-signature such as through the use of a student identification number and password (Foster). Once again though, the risk exists that the person submitting the electronic signature might not be the actual person. If an individual's password is compromised (by hacking or the student himself), then identity verification is much more difficult to be assured of.

Internal IT and/or Enterprise Systems Risks

A college's own IT systems are another potential source for privacy violations. A challenge for universities is ensuring appropriate employee access to IT/enterprise systems. Campus employees include permanent, temporary, or student workers. A flawed system structure or improper access authorization may mean that employees can see student data that is not necessary for their job function. In other cases, employees' access may be compatible with their job responsibilities, but workers may inappropriately use private information for shady purposes. Jennifer C. Wasson points out that there have been court cases where school staff disclosed social security numbers to post office personnel and another where an instructor disclosed a student's HIV condition (5). Even if campus employees do not use or share information, there is always the possibility that they could access private information for their own personal curiosity, which most people would agree is an invasion of privacy.

Another IT system risk is “logging.” Logging is “the process by which a systems administrator collects data about a computer network and the individuals using it” (Wasson 2). Logging is not covered under FERPA, but the practice poses potential privacy concerns since it would enable administrators to monitor student network activity such as Web sites a student visits, email exchanges, and ID card usage. The fear is that schools will act as “Big Brother” by monitoring and tracking student movements.

As with email and e-signatures, IT systems are also exposed to hacking. According to USA Today, 2007 had “139 reported information security incidents around the world, a 68% increase from the previous year” (3a). Chip Shields further states that “[t]he University of Arizona averages 20,000 hits a day from people trying to find vulnerabilities in its network connecting more than 30,000 computers…” (55). Higher education institutions not only need to worry about outsiders hacking in, but also the institution’s own students that are “inside the wall” (Shields 55-56).

Next, since FERPA requires educational records to be accurate, data integrity is an important concern for higher education institutions. For example, Weber State University mandates that “1) accuracy and completeness of all system contents are maintained during storage and processing, 2) system capabilities can be re-established within an appropriate time after loss or damage by accident, malfunction, breach of security, or natural disaster, and 3) actual or attempted breaches of security can be detected promptly and controlled” (1).

Electronic Output and Hardware Risks

One key advantage of information technology is that it allows quick access to vast amounts of information for both students and employees. It also allows flexibility to access data from virtually any location. Students and employees do not have to be anywhere near campus to get the information they want as long as they have online access. Information is now being exchanged in electronic documents through technologies such electronic data interchange (EDI), XML, and GeoTrust (Morley and Ramirez 61). In addition, "there is also vendor application software that extracts information from a student records data base, assembles it into an image file, then emails it" (Morley and Ramirez 61). If universities choose to transmit documents, such as transcripts, via electronic exchange, then security will be of the utmost importance.

Employees could endanger student privacy by handling paper output carelessly and failing to safeguard laptops or home computers. Throwing away sensitive paper items in the trash, or leaving printed records and laptops in unsecured areas leaves such data susceptible to theft. Employees even have to be mindful of leaving paper records in their office if a maintenance person could access it. Regarding laptops and hardware, the National Center for Education Statistics astutely says that institutions "must more *regularly* deal with threats like failed hard drives, spilled coffee, and refrigerator magnets" (1).

FERPA IT Controls

Higher education institutions have several tools to mitigate the aforementioned risks and adequately safeguard data. These include the following:

- Install anti-virus software and firewall protection on all university computers (Shields 55). Require student course systems and Web sites to use Secure Sockets Layer (SSL) protocols. Use service-oriented architecture like UIUC's bluestem to help further protect web sites from unauthorized access (Wood).
- Build "software flag alerts" into employee enterprise systems that explain to users how to view and handle sensitive information (Fratt 1).
- Back up system data and store it off site to help protect data integrity (Shields 55).

- Encourage instructors and administrative staff only to maintain and store the least amount of information related to a staff member's particular educational interest (Hillison et al. 311). Keeping extraneous data only makes securing private information more difficult.
- Establish and enforce email policies. Using encrypted e-mail, and exercising caution about email message content and subject lines will help secure information. Email users should refrain from putting a university identification number or other sensitive information in the subject line. Colleges could also require campus employees to only communicate through university email accounts rather than private accounts like gmail or yahoo. An additional emphasis on privacy is possible via a disclaimer line in e-mail communications (Morley and Ramirez Q80). A sample disclaimer line reads, "[t]he information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking any action in reliance upon, this information by persons or entities other then the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer" (Morley and Ramirez Q80). While such a disclaimer would not necessarily prevent people from forwarding e-mails along to others, it would help toward promoting a culture of privacy, and providing some protection for the sender.
- Require and communicate that employees and students create meaningless passwords, change them every 90 days, and keep them confidential (Shields 55). Higher education institutions must also continually educate students and employees about the importance of keeping electronic identity information private (Wood).

- Use digital certificates or other secure methods that allow files to be exchanged safely (Katz 150).
- Have a basic security audit conducted by an outside expert (Shields 56). External consultants could also assist with security compliance software. Such software allows institutions to automate many compliance actions.
- Implement an institution-wide identity management program (IdM) to ensure that systems are being accessed by the right person, credentials are "valid at the time of access", and the person performing any system actions (whether it is a student or employee) has the authority to do so (Hawkins 84). An effective IdM program involves understanding system risks to identity theft, getting top stakeholders involved, implementing identity protection policies across the organization, and continually training employees (Hawkins 84-85). IdM programs should be included as part of an overall information security program (Choroszy 1).
- Clearly communicate acceptable-use policies related to school computing resources and establish expectations for privacy (Quinn 203).
- Be consistent and proactive with training, education, and policy issues. A good portion of the overall security effort involves using common sense. Privacy breaches occur when people lull themselves into a false sense of security. Colleges need to actively promote their security policies, and emphasize the negative consequences. All employees should also sign confidentiality agreements.
- Assign one or two specific employees respond to certain types of information requests (such as subpoenas) to ensure that the release of particular kinds of data are handled consistently (Nixon 71).

- Use logging to maintain network safety. Although logging poses its own security risks, it could be a powerful weapon in the war on hackers if it is used only for the purpose of monitoring potential network vulnerabilities and not for the purpose of spying on students (Wasson 6).
- Understand the business cases that underlie system technology. Organizations need a good understanding of the job responsibilities of various employees to figure out what kinds of information people need access to. Procedures should allow the institution to alter access privileges "when changes in duties or employment status occur" (Katz 149).

Needed IT controls are numerous and the above controls only provide a sample. In conclusion, when designing and testing controls, institutions should consider the following categories:

- "*prevention* - e.g., by installing locks on windows and doors, threats are prevented from easily accessing buildings and rooms that house your assets
- "*deterrence* - e.g., by training users about the legal consequences of unacceptable use, potential threats that might otherwise consider destructive activities may be deterred
- "*containment* - e.g., by segmenting each separate type of information in your system, even active threats can be limited to the record areas they can find and enter
- "*detection* - e.g., by reviewing records of user activity, commonly referred to as audit trails, unwelcome activity can be uncovered

- “*recovery* - e.g., by preparing and testing a contingency plan, "lost" systems and "damaged" information can be salvaged (or at least losses can be minimized) (National Center for Education Statistics 1).

Does FERPA Go Far Enough, or Too Far?

While FERPA provides several mandates for protecting student data, some believe that it does not go far enough. For example, Wasson believes that logging activities and records should be covered under FERPA. She argues that student activities on computer and identification card networks are part of the educational record, are maintained and stored by colleges, and therefore, qualify for FERPA (2-3).

Others believe that individuals should have the ability to sue for privacy violations under FERPA (Student Press Law Center). For instance, in the Supreme Court case John Doe vs. Gonzaga University and Roberta League, the defendant in the case attempted to sue under FERPA when an education dean disclosed allegations of a student’s sexual assault incident to prospective employers. The allegations were never proven and no criminal charges were filed (Tone and Pitts 2). Although the Court ruled that John Doe did not have the right to sue under FERPA, there have since been attempts in Congress to change the language of FERPA so that lawsuits could be permitted (Student Press Law Center 15).

Others do not believe that FERPA should be amended, but that schools should adopt stricter privacy policies than what FERPA requires. For example, even though institutions are allowed to disclose directory information, limiting directory access could help prevent identity theft. Universities could limit access by requiring an identification number and password to gain access to the directory. In addition, they could let students selectively restrict which data to release rather than employ an “all or nothing” approach to directory information (Orrick 90).

This example shows that, since schools have some discretion over what is classified as directory information, they could opt for a more conservative approach than what is mandated by FERPA. To illustrate, photos and electronic images are not automatically covered under FERPA. Some institutions consider them to be part of directory information while others choose to keep them confidential unless students submit a written release.

Many other people think that FERPA goes too far. Parents are routinely flummoxed that they cannot obtain information about their son or daughter's academic progress (Babey 1). Parents often wonder how they will know if their child is skipping class or experiencing a disciplinary problem. Concerns also exist that FERPA hinders efforts to disclose health and safety risks. The Virginia Tech incident has led to accusations that school employees are sometimes confused about what can and cannot be shared under FERPA (Moehlmann 1). While FERPA allows schools to disclose information when health and safety risks are present, how do staff members adequately assess whether such risks exist or not? Given the rarity of incidents like the tragedy at Virginia Tech, it is not prudent to overreact and make disclosures any time a student exhibits odd behavior. Conversely, no campus counselor, instructor, or advisor would want to keep warning signs to themselves.

There are also concerns that institutions sometimes use FERPA incorrectly. In 2001, a rape victim at Georgetown University wanted to find out the results of her perpetrator's disciplinary hearing. The university told her that she needed to sign a form promising not to discuss information from the hearing; otherwise, Georgetown would not share the results (Student Press Law Center 15). FERPA did not specifically require that such information be kept private, but Georgetown told the student differently. The victim stated at the time, "[t]hey do not want prospective students and parents knowing that rape happens on their ‘safe’ campus…” (Student Press Law Center 15).

The assorted views on FERPA show that there are not any easy answers as to where campuses should draw the privacy line. Since adequately controlling IT risks hinges on sound policies and accurate risk assessment, campuses must weigh the nuances of a variety of privacy issues to come up with the best security plan. They must further weigh the costs versus benefits of implementing security efforts. Costs can include both financial and personal service costs.

Efforts to tighten IT controls on student privacy sometimes have unintended effects on student service. For example, limiting employee access to aspects of the college’s information system can make it more difficult for them to perform their job duties. As an academic advisor, I often experience conflicts between student privacy and student service. Although I can see the academic records of my advisees, the University restricts my permissions. I am not permitted to add any students to my Department’s courses or fix registration access problems for individual students. Instead, I have to forward requests on to other campus units. The turnaround can take anywhere from a few hours to a few days, so I find it frustrating that my students and I have to wait. This is especially true if it is something I know that I could fix in an instant…if only I had access. However, the University restricts my permissions for a reason, as it does with several advisors across campus. It wants to ensure that campus employees like me do not do anything inappropriate and wants to limit hundreds of people from potentially making improper changes.

Conclusion

FERPA compliance and privacy management pose a unique set of challenges for higher education institutions. There is no “one-size-fits-all” approach to safeguarding data and there are no shortcuts. The key starting point to success for any institution is a thorough understanding of its processes, risks, business cases, and vulnerabilities. Without this knowledge, it is impossible to implement the most effective controls. Once controls are implemented, they have to continually be assessed and updated to keep up with changes. The most important aspect is making sure that all students, employees, and stakeholders are all involved. As the NCES says, "*All* employees should participate in security procedures at *all* times" (1). Control implementation efforts must take into account the costs versus benefits, and must also strike a balance between keeping student data private while also enabling effective student service.

Works Cited

Babey, Evelyn R. "Privacy Rights and Perplexed Parents: Proactive Strategies for Institutions." Student Affairs Law & Policy Quarterly. 1:1 (Jul 2004): NA. <http://www.resccu.com/respaper7.html>

Choroszy, Melisa N. "Beyond FERPA: Maintaining the Privacy and Confidentiality of Student Data." <http://www.pacrao.org/docs/resources/writersteam/BeyondFERPA.doc.>

Dillon, Liam. "Ave Maria Web site publicly releases private student records." Naples Daily News. 25 Feb. 2008.

Foster, Andrea L. "Students Can Electronically Authorize Release of Personal Data, Education Department Says." The Chronicle of Higher Education. 7 May 2004: NA. AcademicOneFile. Gale. University of Illinois Urbana-Champaign. 21 Apr. 2008.

Fratt, Lisa. "Virtual Eyes: Higher ed tiptoes into e-mail surveillance." University Business. Nov. 2006. <http://www2.universitybusiness.com/viewarticle.aspx?articleid=605>

Hawkins, Brian L. "What Higher Ed Leaders Need to Know about IdM." EDUCAUSE Review. Sep./Oct. 2007: 84-85.

Hillison, William; Pacini, Carl; and Williams, Paul F. "Confidentiality of student records in the electronic frontier: professors' and administrators' obligations." Journal of Accounting Education. 18 (2000): 301-313.

Jacobson, Jonathan. "E-mail exposes confidential file." The Daily Illini. 27 Aug. 2007.

Katz, Richard N. and Associates. Web Portals and Higher Education. Jossey-Bass. San Francisco, CA. 2002.

Malmgren, Carol. "Primer for Parents: Understanding FERPA as it Relates to Your Student's UIUC Academic Record." www.uiuc.edu. Jan. 2007. <http://www.oar.uiuc.edu/current/parents.html>

Moehlmann, Maximilian. "The Lessons of Virginia Tech." Time. <http://www.time.com/time/specials/2007/article/0,28804,1651473_1651472_1650464,00.html>

Morley, Robert and Ramirez, Clifford. "Q&A Session for Creating a FERPA Friendly Campus Web Conference with Academic Impressions." 26 Oct. 2005.

National Center for Education Statistics (NCES). Safeguarding Your Technology. 98. <http://nces.ed.gov/pubs98/safetech/appendix-b.asp>; <http://nces.ed.gov/pubs2005/tech_suite/part_5.asp>

Nixon, Andrea. “Responding to Compulsory Legal Requests for Information.” EDUCAUSE Review. Mar/Apr 2007: 70-71.

Orrick, Diana Mayer. “Toward Adequate Online Privacy Safeguards.” Computer. Aug. 2002: 92, 90-91.

Quinn, David M. “Legal Issues in Educational Technology: Implications for School Leaders.” Educational Administration Quarterly. 39 (2003): 187-206.

Shields, Chip. “Are Script Kiddies Hacking Your System: How to fight the onslaught of cyber attacks.” District Administration. Nov. 2003: 54-56.

Student Press Law Center. “A Light in the Darkness?” Campus Crime. XXV. No 1. (Winter 2003-2004): 15.

Tone, Joe and Pitts, Lee. “Gonzaga University & League, Roberta v. Doe, John.” Medill – On the Docket. 23 June 2004. <http://docket.medill.northwestern.edu/archives/000625.php>

USA Today. “Securing students’ data top tech issue.” 20 Mar 2008: 3a.

Wasson, Jennifer C. “FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy?” North Carolina Law Review. 81 N.C.L. Rev 1348. Mar. 2003: 1-20.

Weber State University. “Data Standards.” 29 Oct. 2004. <http://departments.weber.edu/qsupport&training/Data_Standards/Data_Integrity.htm>

Wood, Barb. Training Presentation. “FERPA: Protecting the Privacy of Student Information.” 66 Library. University of Illinois. Champaign, IL. Jan. 2007.