The Use of Electronic Data Interchange under the Family Educational Rights and Privacy Act

by Paul T. Rhinehart

Among the many technologies that continue to transform our colleges and universities, one of the latest is electronic data interchange, or EDI. When used in the student records area, EDI allows electronic student records to be fed directly into a receiving institution’s database, instead of being sent by mail. While this process offers many clear advantages, one important question that needs to be addressed is how will students’ privacy be protected under this new means of transmission?

The application of electronic data interchange (EDI) in the area of student records in higher education has been recent and rapid. EDI was first developed for use in banking (the familiar ATM, for example) and the trucking industry, with application in higher education student records transmission emerging in the late 1980s. One pioneer was the Georgia Institute of Technology, which in 1989 started to accept student “flat file” applications for admission electronically. Georgia Tech viewed the process as a method of speeding the application process, reducing time spent in data entry, and also recruiting technically advanced applicants.1

To date there are approximately 459 institutions involved at some stage of EDI implementation. The widest application has been in the task of transmitting transcripts between institutions during the admissions process. For example, in Florida over 250,000 student records are exchanged within the state per year by EDI. The University of Texas at Austin has received over 40,000 transcripts via EDI.2

And the process could very well soon go national. The American Association of Collegiate Registrars and Admissions Officers (AACRAO) has developed a system of EDI known as SPEED/E/ExPRESS and has gained government acceptance for its X.12 standard protocol. This is an important step, in that it provides uniformity in transmission. The Department of Education is also supporting the use of EDI. Further, major organizations such as The College Board and Peterson’s are developing national electronic clearinghouses of student data, for the purpose of transmitting batches of student applications and records, and helping schools and students “find each other.”3

As the use of EDI of student data continues to increase, one concern is the legal protection of privacy afforded students under this new technology. Currently, student record privacy is protected under the Family Educational Rights and Privacy Act of 1974, known as the Buckley Amendment or FERPA.4 However, FERPA, having been written over twenty years ago, does not explicitly address EDI. Thus, college and university officers are left with the following sources for guidance:
• new interpretations of the existing FERPA legislation,

Note: Alphabetical reference annotations refer to code and legal citations, found as endnotes to this article.

Paul Rhinehart (rhinehart@ocean.st.usm.edu) is currently completing his Ph.D. in higher education administration at the University of Southern Mississippi, where he served for five years as an assistant in the office of the Graduate Dean and the Office of Graduate Admissions. He has also served as a research intern with the Educational Testing Service in Princeton, New Jersey.
• extension of principles established in past case law concerning FERPA, and
• the world of electronic banking, where, because of EDI's early application, there are already established procedures, legislation, and case law.

At least one of these sources, past case law concerning FERPA, is especially thin, because there have been very few court cases addressing FERPA. One reason for this is FERPA stipulations which require that the Department of Education's FERPA Office resolve most complaints administratively. Another reason is the absence of any allowance in FERPA for private action and recovery of damages as a result of violation of FERPA protection. Also, given the novel nature of EDI, there is especially a dearth of case law here; traditionally, legislation/jurisdiction experience a time lag behind technological change. The topic is, however, currently being researched by the FERPA office.

EDI of Directory Information

To begin the analysis, there are two categories of student information, according to FERPA (a)(5)(A): “directory” information and “non-directory” information. Directory information consists of students' names, addresses, telephone listings, dates of birth, major fields of study, and so forth, which are already officially available to the public. FERPA (a)(5)(B) does state that the student must have a chance to request non-release of directory information. However, barring such a request, directory information in fact must be made available to the public under the Freedom of Information Act (FOIA).

Thus, as long as student data clearly fall into the category of directory information and the student has not requested non-release, there will be no primary privacy concerns with EDI.

There has been some judicial controversy, however, concerning when certain student data are or are not properly directory information. In judicial rulings concerning this question, the courts attempt to balance FOIA vs. FERPA — the privacy interest of the student is weighted against the genuine need of the party requesting the information for its disclosure.

From the case law, one can discern the following guidelines for circumstances when directory information is not disclosable:

1. When student information is matched with achievement test scores. The test scores themselves must be disclosed; however, names and social security numbers must be presented in a masked and scrambled format.

2. When it accompanies other student statistical data, in this case number of transfer students, exams taken for transfer purposes, and sponsoring schools. Again, the school must release the statistics, but without names and addresses or other personally identifiable information.

3. When the school has not published policy of release of directory information, as required under FERPA. Said the Supreme Court of New Hampshire, student name and address data are protected as an extension of the privacy of the home as protected under the fourth and fifth U.S. Constitution Amendments, and release of this data would place the children "at the mercy of pedophiles and other criminals who could do them harm."

Further cases have provided the following:

• Social Security numbers do not constitute directory information. However, FERPA (b)(1)(D) allows the school to release identifiable individual data, even including course grades, without consent to an employer who sponsored the student in the course.

• Information concerning the funding of individual athletic students is not "educational records" protected by FERPA. An athletic conference is not an "educational agency," and so is not subject to the authority of FERPA.

Presumably, such distinctions as are made in the above cases are independent of the mode of transmission, and so would be applied exactly the same under EDI. The only difference may be that with EDI the question of privacy protection will perhaps become more intense because of:

1. the sheer increase in volume of data transmitted,
2. its concentrated possession by central clearinghouses, with the data's obvious value to marketers.

EDI of Nondirectory Information

There is more reason to be concerned about the use of EDI with respect to the release of nondirectory information. Nondirectory information is not public knowledge under FERPA, and so its privacy is guarded much more closely. There are several provisions of FERPA which would be of particular interest under EDI.

Will written consent be required?

First, one of FERPA's major concepts is that no nondirectory information should be disclosed without written permission of the subject (or parents) [(b)(1)]. However, since most use of EDI takes place within the admissions process, technical permission is not required. This is because, according to FERPA (b)(1)(B), there are several exceptions to the consent requirement, among them: release of data to "officials of
"Now, extending the application of EDI yet further, assuming that the school does obtain consent, must such consent really be "written"?"

Thus, transcripts could be sent without any prior written consent. The institution to which the student had applied could merely request the information on its own from the source institution. If this were to occur, the source school would still have to observe the following FERPA stipulations protecting the student's privacy: the school must publish its policy of what it will release and to whom; the student must have a chance to request non-release; and the student must receive notice each time information is sent.

Nevertheless, even though it is not technically required, most institutions will most likely seek some form of written consent from the student. In fact, under the current process, most institutions require students' written consent each time a transcript is requested. This process seems to result from the fact that the school collects a fee for each transcript, and there is no established popular procedure by which one institution directly requests a transcript from another.

Prospectively, however, when EDI is brought into the picture, there is yet another reason that schools may wish to require written consent—namely, there is the problem of the as-yet-unproven and possibly risky method of transmission. Thus, the school may wish to have the student sign a waiver referring to the electronic mode of transmission, with language to the effect that, "I give the institution permission to release my transcript electronically to requesting educational institutions." Indeed, the original AACRAO Legal Guide of 1984 includes a whole addendum of such canned clauses, and similarly the Electronic Fund Transfer Act (EFT) of 1978 provides for the Federal Reserve Board to issue such canned clauses for banks to include in signed documents.

Could electronic consent be used?

Now, extending the application of EDI yet further, assuming that the school does obtain consent, must such consent really be "written"? The question arises because in order to deploy EDI to its fullest advantage, one would envision a situation of electronic consent. However, this threatens the very aspect of FERPA which requires that the consent must be written, i.e., by signature.

It would be very convenient, indeed, for the institution to be able to accept authorization via electronic communication with the student, and so the question arises of what exactly could suffice as official authorization. The use of paper by mail in today's modern age is beginning to seem ever more inconvenient to today's consumers, including students, who are used to faster means such as ATM bank machines.

According to FERPA officials, the law as it now stands requires a paper signature. However, the trend may be toward the acceptance of electronic verification procedures, such as passwords, as modeled on the emerging use of such passwords in electronic fund transfers (EFT) and ATM use in banking.

Obviously, this creates definite security questions, as it somehow seems less secure to rely on the secrecy of a password or PIN number (as employed in many colleges and universities in telephone registration systems) than a written signature. (But one wonders, with the pace of technology, will signatures be able to be collected by means of people writing with electronic pens on the screen itself, as used in the Apple Newton, for example?)

Indeed, if FERPA were to be construed along the lines of the EFT Act, it would allow the legality of passwords for discrete transactions. Under the provisions of the EFT Act, written means do still play a part, but more as a kind of meta-authorization signed by the customer very early in the
relationship and stating procedures by which all subsequent recurring transactions will proceed. For example, when you obtain an ATM card, you sign a document covering the relationship, and then each transaction is carried out with a password.

Considering privacy protection, it is also significant that such an electronic authorization system would not be without backup, because FERPA demands student notification of each transaction, so that the student would notice if something went wrong. Similarly, the EFT Act includes multiple extra security provisions, such as requiring a written record to be generated for the customer during each transaction (the printout generated by the ATM); a regular (usually monthly) list of all transactions; and procedures for corrections of mistakes. Similar provisions could be added to FERPA.

By the way, in any discussion of EDI, the question arises of access and fairness for students on rural or poor areas, and in fact in this regard the EFT Act does provide that at no time can it be mandatory that the customer employ electronic means for the transaction.

Given acceptance of electronic authorization, then, the scenario could work as follows: at the inception of her relationship with the institution, the student could be issued an electronic password or card, similar to an ATM number or a personal ID number for telephone registration, and all subsequent actions could be carried out by computer, including transcript requests.

**What about system security and liability?**

Finally, and perhaps most tangibly important for the institution itself, assuming that electronics are used both for authorization by means of password and for the transmission itself, the question remains, is the system itself, the data in transit, secure? And at what level will the institution have to prove its security or face liability?

Oddly enough for a piece of legislation concerned with protecting privacy, FERPA nowhere explicitly stipulates the duties of the institution to ensure the minimum inherent security of the data storage and transmission system itself (presently the filing cabinet and federal mail system). Rather, the legislators seem to have left this merely to be implied.

This void in the legislation is beginning to seem a bigger problem. First, there is very scant enforcement even under the current paper system. For example, currently registrars never take the time, and indeed could not take the time, to verify every signature they receive on mailed transcript requests. Also, with the increasing use of facsimile (fax) machine requests, there is document distortion and signature distortion by such means. If we accept payment by VISA card number, how do we know who is sending us this number? What if someone’s password is stolen?

These kinds of questions are gaining increasing attention. According to a FERPA official, these issues are of currently heated debate in the use of EDI for student loans and financial aid.

As we move toward EDI, indeed, the means seem less secure. Several writers address the vulnerability of EDI. For example, Willis H. Ware is concerned about “hackers” obtaining data:

Between the outreach of remotely provided computing services and the interconnectivity of modern day networking, the educational community finds itself in an ever increasing posture of exposure and subject to an increasing scope of threats: fraud, hacking, pirating of information, stealing of computer resources, destruction of records, invasions of privacy, physical damage to facilities … 14

And Curran says,

Many computer systems presently in use do not sufficiently protect the privacy concerns required in Buckley and other privacy laws. Courts have made it clear that efforts to blame the computer will fall on deaf ears. [The threat is] risk of deliberate tampering. 15

Further, Goode and Johnson note the possibility of accidental diversion of data across lines, simply because of glitches in the system. 16

Perhaps most significantly, the courts too have recognized this danger. For example, in the court’s ruling in Wachter v. Denver National Bank, 17 the U.S. District Court, applying the EFT Act, stated that because electronic transmission was new, expanded legislation had become necessary to “alleviate concern” and to “enumerate rights and responsibilities.” The court further said that the EFT Act was meant to protect customers, in light of the idea that automated systems are “more vulnerable to fraud and unauthorized use” than traditional methods. These same concerns would seem to be relevant now in the situation of EDI of student records.

Indeed, under FERPA and under future EDI rulings it will be an important issue as to what constitutes “enough” or “reasonable” measures for the institution to protect EDI transmissions against hacking and privacy invasions. 17

Such liability was upheld in the case of Bradford Trust Co. v. Texas American Bank, 18 where the court ruled under an application of the Consumer Credit and Protection Act 19 that a bank was liable for failure to follow its own “internal

---

13 Ibid.
15 Curran, p. 17.
16 Goode and Johnson, p. 61.
17 Friedenberg interview; interview of FERPA official; Palmer and Wei official; interview of FERPA official; Palmer and Wei, p. 9.
Several court decisions have ruled that there is no right for individual private action and recovery of damages as a result of violation of FERPA protection.

Would EDI FERPA violations be litigated?

The only remedy that FERPA itself provides for violations is the withdrawal of federal funding. According to the courts’ interpretation, in order to be punishable such violations must be on a systematic, not an individual, basis, and must be handled via administrative procedures by the FERPA Office in the Department of Education. Said the U.S. District Court in Smith v. Duquesne University: “[I]t is clear that FERPA was adopted to address systematic, not individual, violations of students’ privacy ... to stem the growing policy of many institutions to carelessly release student records.”

Curran, however, points out that no institution has ever been penalized with loss of federal funding; rather, under finding of a violation the Department of Education merely brings the offending institution into future compliance. He does, however, suggest the possibility of individual suit under tort law. Further, some courts have found that there may be cause for private relief under application of Section 1983.

Several court decisions have ruled that there is no right for individual private action and recovery of damages as a result of violation of FERPA protection. The courts’ reasoning here is based on the absence of any allowance for private action in FERPA itself, and on similar court precedents related to other similar federal legislation.

Further, as Curran points out, there is no private right to action because the right to privacy is not a right recognized by the federal Constitution. The U.S. Constitution never mentions the word “privacy.” However, Curran notes that the individual’s right to privacy is hinted elsewhere in the Constitution, which “speaks of other privacy-related rights—the right to be free from unreasonable searches and seizures, and the basic right of liberty protected by the due process clauses of the fifth and fourteenth amendments.”

On the other hand, one of the more important cases to date on this point, Porten v. University of San Francisco, does seem to leave the door open for private suit under at least two possible scenarios:

1. The court seemed to imply that there would be a possibility for private suit based on tortious invasion of privacy, if the unauthorized disclosure were “to the public in general or to a large number of persons,” rather than on a more limited scope.

2. The court in Porten acknowledged that where the state constitution provides the explicit right to privacy, such a right becomes “inalienable,” “self-executing,” and “confers a judicial right of action on all [citizens].”

Again, should there be future FERPA legislation modeled on banking regulations, the institution may be required to ensure “reasonable care” in establishing security of records, and be liable for failures, as banks are under the Bank Secrecy Act, and for example, Bradford v. Texas American Bank.

And lastly, as regards any “hackers” who may perpetrate the illegal interception of transmissions, there may be penalties for them. For example, the Electronic Communication Privacy Act of 1986 covers the illegal interception of transmissions, by phone, TV, or computer, with civil and criminal penalties up to a $10,000 fine.

The Future of FERPA and EDI

The possibility is that we will need amendments to FERPA to address the new technology. According to Curran, “Unfortunately, the new regulations ... of 1988 do not address the issues of computer records ... Buckley needs an electronic overhaul to bring it into compliance with modern electronic systems.” In addition, certainly case law interpretations will emerge constraining FERPA in the context of EDI.
Interestingly, at least one constitutional law expert has actually suggested a federal Constitutional amendment to extend all current individual protections into the new world of technology. Laurence Tribe proposes a “high-tech” amendment to provide “constitutional protections construed without regard to medium.”

As for future scenarios, there has been some speculation about the possible national societal implications of EDI. Among its ramifications might be the de facto formation of a quasi-national “universal university.” As institutions increasingly communicate using a standardizing network, it is logical to suspect that their respective internal operations may also tend to become standardized. Such a “universal university” system could be heavily dominated by the large public universities, and may “swallow” smaller private institutions, who would be unable to compete with resources, and whose market identity differentiation could become less feasible.

In fact, these possibilities and other scenarios like them were the concern of the EFT legislators. Part of the EFT Act created a body to further investigate and report back to the legislature concerning possible impacts of EFT on the smaller banks, on competition within banking, and on access by those of low income. All of these concerns have their equivalents in the area of EDI in student records, and may well be a focus of concern in the future.

Code and Legal References:

- Zaal v. State of Maryland, 602 A.2d. 1247 (Md. 1992)
- Arkansas Gazette Co. v. Southern State College, 620 S.W.2d. 258 (Ark. 1981)
- 751 F.Supp. 906 (D.Colo. 1990)
- 790 F.2d. 407 (5th Cir. 1986)
- U.S. Code, vol. 18, secs. 1367, 2232, 2510 et seq., 2701 et seq., 3117, 3121 et seq. (1988)

Privacy of Student Information
in a Networked Information Environment:
Beyond FERPA and EDI

With the proliferation of campus connectivity to the Internet and networking of information, many questions are arising related to the privacy of student information:

- Can rosters of students enrolled in classes be posted on the World Wide Web?
- Is our institution liable for a violation of privacy that occurs because of information posted on a student’s Web page when we have no policy regarding what students may post?
- Which administrators should have access to which data?
- Can student photos be posted to an electronic directory?
- What does “secure” mean in an Internet environment?
- Can we use e-mail to deliver student course and billing information?
- Given that some listserv software can be queried to determine who the subscribers are, is this a violation of FERPA protections for “academic records”?

CAUSE, in cooperation with the American Association of Collegiate Registrars and Admissions Officers, has created a task force to develop a white paper that will provide guidelines to help colleges and universities create or refine policies and processes related to the collection, use, maintenance, and disclosure of personal information of students in an increasingly networked environment. These guidelines will evolve through a thorough review of applicable state and federal laws, emerging legal questions, current campus incidents, relevant literature, and existing campus policies, and through an understanding of the concerns of stakeholders such as bursars, admissions officers, financial aid officers, and registrars. The paper will articulate the continuum of values that influence the creation of policy, and take into account the advances and implications of the technology that raises these issues.

Task Force Membership

Co-Chair:
Virginia Rezmierski
Assistant for Policy Studies
to the Vice Provost for IT
University of Michigan

Kathleen R. Kimball
Computer Network and
Information Security Officer
The Pennsylvania State University

Robert Morley
Associate Registrar
University of Southern California
(Morley chairs the AACRAO SPEEDE Committee and represents AACRAO on the task force)

Co-Chair:
Susan Stager Ferencz
Director of Policy and Planning
Office of Information Resources
Indiana University

Robert Morley
Information Security Officer
Computer Network and
The Pennsylvania State University

Laurence Alvarez
Associate Provost
The University of the South

Trang Pham
Public Policy Graduate Student
University of Michigan

Clair W. Goldsmith
Deputy Director
Academic Computing Services
University of Texas, Austin

Robert Ellis Smith
Publisher
Privacy Journal

Steven L. Worona
Assistant to the Vice President for IT
Cornell University