

STUDENT PRIVACY: FROM FACEBOOK TO FERPA  
June 25-28, 2006

Phyllis Karasov  
Moore, Costello & Hart, P.L.L.P.  
Saint Paul, MN

Steven J. McDonald  
Rhode Island School of Design  
Providence, RI

Margaret O'Donnell  
The Catholic University of America  
Washington, D.C.

I. The Security of Education Records Stored in University and Personal Computers.

A. FERPA and Electronic Information.

1. Clearly, information related to a student that is maintained within a college or university computer system, which does not fall within any of the listed exceptions, meets the definition of "education records" under FERPA.
2. In 1996, the term "record" was amended to add "computer media" to the definition of record, in addition to information recorded by handwriting, print, video, audio tape, film, microfilm and microfiche. See 34 C.F.R. § 99.3.
3. E-mail messages may fall within the definition of "education records" provided the message is "maintained" by the institution. In President and Trustees of Bates College v. Congregation Beth Abraham, 2001 WL 1671588, (Me.Super., February 13, 2001), the court stated:

"The e-mail messages here were generated by students and directed to the faculty advisor . . . The records directly related to the named students and sought the advice and assistance of a person acting for the college. Although the e-mail correspondence may be of a different character than most records, files and documents maintained by an educational institution, [FERPA] does not limit the definition of [education records]. As such, that term ought to be liberally construed to be inclusive rather than exclusive to carry out the Act's purpose and intent for the protection of the students."

4. Obviously an e-mail message that is sitting on a student's own computer is within the control of the student because the student is not maintaining the message on behalf of the institution. See Owasso Independent School District v. Falvo, 534 U.S. 426, 122 S. Ct. 934 (2002). On the other hand, if a university employee, such as an IT employee has access to the message, it becomes an education record within the definition of FERPA.
5. If e-mail messages posted to a class list serve or web page are open and available to anyone who reads the list serve or web page, the e-mail messages may not be considered to be covered by FERPA. Even if the list serve or web page is deemed to be covered by FERPA, there may be implied consent to disclosure. This situation may be analogous to allowing students to post messages on a bulletin board. On the other hand, if a faculty member actively manages the list serve or web page, or students are required to post the messages, the e-mail messages might be covered by FERPA.
6. If an institution includes e-mail addresses in the information it designates as directory information, then e-mail messages can be disclosed without prior consent, unless a student has objected to disclosure of his or her e-mail address as directory information. See 34 C.F.R. §§ 99.3, 99.31(a)(11) and 99.37. See also 65 Fed. Reg. 41852, 41855 (July 6, 2000) where the Department of Education stated: “[A]s methods of communication and record management continue to evolve, it is useful to list additional categories of information that we believe are directory information, such as a student’s e-mail address . . . We do not believe that the disclosure of student e-mail addresses will generally be considered harmful or an invasion of privacy. We think that a student’s e-mail address is analogous to a student’s mailing address, an item already included as directory information.”
7. In 2004, 34 C.F.R. § 99.30 was amended to accommodate written consent provided by e-mail. § 99.30(d) provides that “signed and dated written consent” can include a record and signature in electronic form that:
  - (1) identifies and authenticates a particular person as the source of the electronic consent; and
  - (2) indicates such person’s approval of the information contained in the electronic consent.

This means that institutions can honor electronic signatures for release of records to the student or to a third party, such as releasing a transcript to another school.

- a. It is unlikely that an e-mail request, without additional information to identify and authenticate the student as the source of the electronic consent, will meet this definition of signed and dated written consent.
  - b. Instead, the school should develop a procedure to require additional identifiers online. For example, requiring an I.D. number and a password to identify and authenticate the person.
8. As of April 28, 2006, according to the Privacy Rights Clearinghouse, there have been data security breaches in 24 institutions of higher education.

B. Disclosure of Student Identifiers

1. “Personally identifiable information” is defined under FERPA as including, but not limited to, the following information:
  - a. The student’s name;
  - b. The name of the student’s parent or other family member;
  - c. The address of the student or student’s family;
  - d. A personal identifier such as the student’s social security number;
  - e. A list of personal characteristics that would make the student’s identity easily traceable;
  - f. Other information that would make the student’s identity easily traceable.
2. One of the exceptions to the disclosure of personally identifiable information from education records without prior consent is disclosure to school officials with legitimate educational interests. 34 C.F.R. § 99.31(a)(1).
3. An institution of higher education can designate individuals from its alumni office as a “school official.” Thus it would be permissible for a school to share student identifiers, as well as directory information, to an alumni office.
4. On July 25, 1996, the FPCO issued a letter to Vermont Law School responding the following question:

“Is there, in turn, anything that prevents the alumni office from providing select social security numbers, as the need arises, to outside organizations that provide a search for current addresses using this information”?

In the advisory letter, the FPCO indicated that if the alumni office has a contract or written agreement with an outside organization that is

providing a service for an institution of higher education, such as searching for current addresses of its students, it is permissible for the alumni office to disclose student identifiers, including social security numbers, to that organization, without prior written consent of the students. Obviously, FERPA limits the redisclosure of information from education records by third parties that receive such information. See 34 C.F.R. § 99.33.

5. In an [advisory opinion to the University of Wisconsin - River Falls, dated November 5, 2004](#)<sup>1</sup>, the FPCO again discussed student identifiers. In that letter, UW-River Falls used an account I.D. number which is a randomly assigned seven digit number that is not based in any way on an individual's social security number. UW-River Falls asked if the students' account I.D. number could be disclosed as "directory information."

The FPCO stated that "FERPA allows an institution to designate and disclose as "directory information" a unique personal identifier, such as a student's user or account logon I.D. (or an e-mail address used as a logon I.D.) as long as the identifier cannot be used, standing alone, by unauthorized individual's to gain access to non-directory information from education records.

"In other words, if a student must use a shared secret, such as a PIN or password, or some other authentication factor unique to the student, along with their personal identifier to gain access to their records in the student information system, then that identifier may be designated and disclosed as directory information . . ."

"Conversely, if an institution allows students to access [their] own education records using a personal identifier but without the use of a password or other factor to authenticate the student's identity (or if the identifier itself is also used to authenticate the student's identity) then that identifier may not be disclosed as directory information under FERPA because it could result in the disclosure of protected information to someone other than the student and thus would be "harmful or an invasion of privacy if disclosed" . . .

### C. Disclosure of Education Records Relating to a Deceased Student.

1. FERPA generally protects an eligible student's privacy interests in "education records." The term "education records" is defined as records

---

<sup>1</sup> Letters cited in this paper which are available on the Family Policy Compliance Office web site are hyperlinked to their location on the web site. If you are not reading this document in electronic form, the cited letters can be found at <<http://www.ed.gov/policy/gen/guid/fpc/index.html>> under either "Online Library" or "Hot Topics", unless otherwise noted.