November 5, 2004

Ms. Judy George, Registrar
University of Wisconsin-River Falls
410 S. Third Street
River Falls, WI 54022

Gary S. Smith, Ph.D., Chief Information Officer
& Director of Information Technology Services
Ms. Mary-Alice Muraski, eSIS Project Director
University of Wisconsin-River Falls
410 S. Third Street, North Hall 139
River Falls, WI 54022-5001

Dear Ms. George, Ms. Muraski, and Dr. Smith:

This responds to Ms. George's email dated May 18, 2004, and Ms. Muraski's and Dr. Smith's June 20, 2004, letter and follow-up email dated August 2, 2004. Collectively, you asked whether in the circumstances you described a student's "account ID number" can be disclosed as "directory information" under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g. This Office administers FERPA and is responsible for investigating complaints and providing technical assistance to ensure compliance with the statute and regulations codified at 34 CFR Part 99.

We have advised previously that a student ID number, like a student's social security number (SSN), may not be designated and disclosed as "directory information" under FERPA. It appears that this has created some confusion or concern on your part about what actually constitutes or defines a "student ID number" for purposes of this guidance. You explained that the problem arises because many commonly used technologies, such as campus portals and single sign-on approaches to information systems, as well as electronic communication systems, require publication of the personal identifier used by students to access the system.

According to your communications, the account ID number in question is a randomly assigned, seven digit number starting with the letter "W" that is not based in any way on an individual's SSN. The University's student information system (known as "eSIS") requires a student user to enter this number and a secret password in order to enter eSIS and access the student's own education records. The University also assigns each student a unique email address. Following the practice of many institutions, the University has ceased using student SSNs for any of these purposes.

The University provides students with an eSIS account ID number when they are accepted for admission, and this number remains assigned to the same student throughout his or her relationship with the University. Students use a web page to activate the number by providing their assigned account ID number, their date of birth, and the last four digits of their SSN. Once authenticated in this manner, the student must choose from a list of randomly generated passwords and establish and answer a security question, such as "What is your mother's maiden name?" Students may change their passwords after logging into the same web page and providing their existing password and the answer to their security question. A student who forgets his or her account ID number can obtain a new one from any of several functional offices, such as Admissions or Registrar.

A school official with an appropriate need to know who wishes to access a student's record must first login to eSIS using his or her own unique account ID and password. Once properly authenticated to the system, the school official may access a student's record by entering the student's account ID number, if known, or the student's name. Dr. Smith indicated that a school official might know a student's eSIS account ID number if the student had provided it or if the number was listed on an internal document. Dr. Smith explained further that the University uses the system's access control features to allow school officials to access a student's records only to an extent consistent with their professional role and responsibilities. For example, a staff person in the Housing Office would only get to see information pertinent to housing matters, whereas someone in the Registrar's office would most likely be allowed to see a greater range of information.

Dr. Smith and Ms. Muraski stated generally that the "directory-based identification and authentication tools that are utilized in these [self-service oriented technological] environments are structured such that it is essentially impossible to effectively hide the logon or access I.D." In response to follow-up questions from this Office, Dr. Smith explained that the eSIS account ID number cannot effectively be made private because it is the key that is used to identify the student in the LDAP (Lightweight Directory Access Protocol) directory server and software. In order for eSIS to return correct information, the account ID number must be verified against the LDAP directory, which in turn is queryable by those with access to the server regardless of their status as school officials with a legitimate educational interest. (Passwords, in contrast, are protected against disclosure through a system query.)

According to Dr. Smith, an eSIS query with the name of a student who has not blocked directory information disclosures under FERPA returns the student's seven-digit, eSIS account ID number along with the student's postal address, telephone number, email address, and affiliation (e.g., student). A system query using the name of a student who has blocked the release of directory information under FERPA returns nothing other than the data that was submitted. While the system is capable of blocking the display of a student's eSIS account ID, those who exercise this option disenfranchise themselves from the conveniences of many self-service activities and may eliminate themselves entirely from participating in certain services where display of this unique electronic identifier is required.

Discussion

FERPA provides that an educational agency or institution may not have a policy or practice of disclosing education records, or personally identifiable information from education records, without the prior written consent of a parent or eligible student, that is, a student who is 18 years of age or attends a postsecondary institution. 20 U.S.C. § 1232g(b)(1) and (b)(2); 34 CFR §§ 99.3 ("Eligible student") and 99.30. The term "education records" is defined as information that is directly related to a student and maintained by an educational agency or institution, or a party acting for the agency or institution. 20 U.S.C. §1232g(a)(4); 34 CFR § 99.3 ("Education records"). Records that are directly related to a student, such as the student's course registration, grades, transcript, housing assignment, and financial assistance, as well as the eSIS account ID number itself, that are maintained by the University constitute "education records" under FERPA.

The term "personally identifiable information" is defined in the regulations as:

(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 or student number;
(e) A list of personal characteristics that would make the student's identity easily traceable; or
(f) Other information that would make the student's identity easily traceable.

34 CFR § 99.3.

"Directory information" is defined as information contained in an education record that would not generally be considered harmful or an invasion of privacy if disclosed and includes a student's name, address, telephone listing, email address, and other types of information about the student. 20 U.S.C. § 1232g(a)(5)(A); 34 CFR § 99.3. An institution that wishes to disclose directory information must comply with the procedural requirements set forth in § 99.37 of the regulations, which allow an eligible student to refuse to allow an institution to disclose directory information about the student.

A student's name and address, which are defined as "personally identifiable information" under FERPA, are also defined as "directory information" because these items are generally made available in public directories outside the school context and otherwise are not considered harmful or an invasion of privacy if disclosed. The legal conclusion in FERPA that these items of personally identifiable information are not considered "harmful or an invasion of privacy if disclosed" is based on an understanding that they generally cannot be used, standing alone, to obtain sensitive, non-public (i.e., non-directory) information about an individual.

In contrast, SSNs, also listed as "personally identifiable information" under FERPA, are often used to obtain a variety of sensitive, non-public information about individuals, such as employment, credit, financial, health, motor vehicle, and educational information, that would be

harmful or an invasion of privacy if disclosed. (SSNs may also be used in conjunction with commonly available directory information to establish fraudulent accounts and otherwise steal a person's identity.) For these reasons, as noted above, this Office has routinely advised that a student's SSN is the kind of personally identifiable information that *may not* be designated and disclosed as directory information. We have generally included "student ID numbers" in the same category because these numbers have historically been used much like SSNs, that is, as unique identifiers used by themselves to obtain access to non-directory information about a student, such as education records (or educational services).

Clearly, there are circumstances, such as electronic mail communications, in which institutions must assign each student a unique personal identifier that can be made available publicly. Indeed, the FERPA regulations were amended in 2000 to include a student's email address in the definition of "directory information." Similarly, as you described, many institutions have established or seek to establish portals and single sign-on approaches to student information systems, or use directory-based software and protocols for electronic collaboration by students and teachers, both within and among institutions, that require some form of public dissemination of a unique personal identifier. It is also well-known that public key infrastructure (PKI) technology for encryption and digital signatures requires wide dissemination of the sender's public key. These are the types of circumstances in which institutions may need to publish or disclose a personal identifier other than a student's name and address.

We believe 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 ID (or an email address used as a logon ID), as long as the identifier cannot be used, standing alone, by unauthorized individuals 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 under FERPA in accordance with the requirements of § 99.37 of the regulations. (Allowance is made for school officials to use the student's published personal identifier alone, just as they use a student's name, to obtain access to the student's education records, provided the school official has a legitimate educational interest in accordance with § 99.31(a)(1) of the regulations.)

Conversely, if an institution allows students to access 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." (Some institutions may continue to use a student's "official ID number" in this manner.) Under this reasoning, an institution that allows a student (or any other party, for that matter) to obtain access to education records by providing just publicly available information, such as a student's name or published email address, without any additional proof or authentication of identity, could have a policy or practice in violation of FERPA because it could lead to the disclosure of education records to unauthorized recipients.

Finally, it should be clear that the standards set forth in this guidance pertain only to the public disclosure of information that identifies a student as part of a computer-based information system that is used to provide directory information on students and allow authorized users to gain access to education records. These standards do not apply to and are not intended to modify in any way the requirements for electronic consent to the disclosure of education records as set forth in § 99.30(d) of the regulations. That is, a student's email address, user ID, logon ID, account number, or any other personal identifier may not be used as an electronic signature unless it meets the specific requirements in 34 CFR § 99.30(d).

In summary, the University may designate and disclose as "directory information" a student's account ID number or other personal identifier used to logon to eSIS provided that it cannot be used, standing alone, by an unauthorized individual to obtain non-directory information from education records.

I trust this responds adequately to your inquiry and thank you for bringing this matter to our attention.

Sincerely,

/s/
LeRoy S. Rooker
Director
Family Policy Compliance Office