CRS Reports & Analysis

Legal Sidebar

What Happens if Johnny Hacks His Seventh Grade Report Card?

12/01/2016

This is part one of a two-part series discussing federal law and education records. This post will address the extent to which the Family Educational Rights and Privacy Act (FERPA) addresses data security for education records. Part II will consider FERPA and privacy concerns raised by the expanded use of computers to collect, maintain, and analyze education records.

In years past, a student's education records were likely to be memorialized on paper and stored in a principal's locked file cabinet. Today, these records can be stored digitally in a computer "cloud" and accessed through the Internet. While digitizing records can increase efficiency, this method of storage has resulted in hundreds of instances of unauthorized access to digitized education records by "hackers" and other unauthorized persons. While there are specific instances in which education institutions may be subject to data security requirements (such as protection of personal financial information), there are no comprehensive federal laws regarding data security of education records.

The Family Educational Rights and Privacy Act of 1974 (FERPA) and its accompanying regulations, which are administered by the U.S. Department of Education (ED), focus on the closely related issue of education records privacy, directing when and how education records may legally be released. Under FERPA, educational agencies and institutions that receive federal funds must have a policy or practice of not releasing a minor student's education records (the definition of which is discussed in Part II) without written consent by a parent. These entities must also provide parents access to a student's educational records (rights that are transferred to a student when that student is no longer a minor). Although there is no private right of action under FERPA, a wronged party may file a complaint with ED. The only enforcement mechanism for FERPA violations, however, is the withdrawal of federal education funds from the institution by ED.

So what happens if Johnny hacks his seventh grade report card (besides his own possible criminal liability)? FERPA was passed when the Internet was in its infancy and computer security data breaches were uncommon. Therefore, the statute does not specifically contemplate the prevention of the breach of educational records. For instance, ED has noted that FERPA does not provide ED the authority to require that parents (or students who are no longer minors) be notified when unauthorized access to education records has occurred. But there are relevant ED regulations. FERPA requires that an educational agency or institution maintains a record of any disclosure of a student's education records. ED has determined that this requirement applies whether or not a disclosure is authorized, and thus, education agencies or institutions are required to record an incident of unauthorized access to computerized education records. Thus, a parent or student may only become aware of an unauthorized disclosure during an inspection of a student's education record.

Furthermore, FERPA itself does not specify methods by which educational agencies or institutions should secure their education records against unauthorized access. ED does, however, encourage education agencies and institutions with digitized education records to consider mitigating any actions that would risk the release of information that can be used to establish a person's identity (personally identifiable information or PII).

FERPA also contains various exceptions under which education records may be released to third parties, and some of these third parties may be subject to data security requirements. Because these third parties are often not recipients of

federal funds, however, the education institution or agency that releases the information bears the ultimate responsibility to ensure the security of the education records. Two exceptions regarding disclosure of education records without the consent of parents are most relevant here.

First, education records can be released to an authorized representative of the Comptroller General of the United States, the Secretary of Education, or state educational authorities (hereinafter FERPA-permitted entities). This authorized representative may obtain education records in connection with 1) an audit and evaluation of federally supported education programs; 2) the enforcement of federal requirements of such programs. Under this exception, FERPA requires that "any data collected by [FERPA-permitted entities] shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements." ED further provides that a state, local education authority (LEA), or FERPA-permitted entity is responsible for using "reasonable methods" to ensure to the greatest extent practicable that any entity or individual designated as its authorized representative protects PII from further disclosures or other uses.

FERPA specifically contemplates that an authorized representative of a FERPA-permitted entity can be a person or entity that is not an employee of a state, LEA, or FERPA-permitted entity, such as a third-party vendor. Information disclosed to such vendors must "[b]e protected in a manner that does not permit personal identification of individuals by anyone other than the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) and their authorized representatives...." If an "authorized representative" is not an employee, there must be a written agreement to designate such authorized representative. This contract must describe policies and procedures "to protect personally identifiable information from ... unauthorized use ...."

Second, educational agencies or institutions, states, or a FERPA-permitted agency may disclose or redisclose education records to third parties in order to conduct studies to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. This information may only be disclosed pursuant to a written agreement with the organization conducting the study. The written agreement must require, among other things, that the organization conduct the study in a way that does not enable the personal identification of students or parents by anyone other than a representative of the organization with a legitimate interest. ED suggests that these agreements should contain specific requirements regarding security protocols to protect educational records, including breach notification requirements.

In the 114th Congress, several bills that were introduced to amend FERPA to address student privacy issues also contained provisions addressing computer security. For instance, S. 1322 would require that educational agencies or institutions receiving federal funds implement information security policies and procedures and require outside parties to whom they disclose education records to have a comprehensive security program. Similarly, H.R. 3157 would require educational agencies or institutions to establish computer security practices for both records held internally or collected by outside parties on their behalf.

Posted at 12/01/2016 10:28 AM

CRS Reports & Analysis

Legal Sidebar

Who Can See Johnny's Second Grade Report Card?

12/01/2016

This is part two of a two-part series discussing federal law and education records. This post will consider the Family Educational Rights and Privacy Act (FERPA) and privacy concerns raised by the expanded use of computers to collect, maintain, and analyze education records. Part I focused on the extent to which FERPA addresses data security for education records.

In years past, when students did classwork, took tests, or interacted with teachers, it was generally done face-to-face or in writing. Today, a student is likely to perform many of these tasks while sitting in front of a computer. Computers can increase the ability of students to communicate with teachers and peers, access educational content, and perform research, while allowing teachers to organize their classes, track their students' work, and evaluate their students' progress. In addition, by accessing the information generated by students and teachers, digital technology can be used by states and the federal government to analyze the effectiveness of teachers, educational institutions, and government programs.

While various state and federal laws concern the gathering and disclosure of student data, changing technology has presented challenges as to how these laws are applied. Privacy concerns have been raised, for instance, regarding how these laws are applied to the collection, storage, and use of education-related digitized information. In particular, the question arises as to whether the law adequately addresses hardware, software, and off-site data storage used by schools but provided by private companies under contract. Also, as educational data collected by schools is more widely used to evaluate the effectiveness of educational programs, the adequacy of existing law with regard to state agencies and their contractors performing these evaluations has been questioned.

Under the federal Family Educational Rights and Privacy Act (FERPA), educational agencies and institutions that receive federal funds must have a policy directing that student "education records" may not be released without the written consent of parents, or, if the student is no longer a minor, the student. Under FERPA, "education records," with some specified exclusions, are broadly defined to include those records, files, documents, and other materials that 1) contain information directly related to a student and 2) are maintained by an educational agency or institution or by a person acting for such agency or institution. FERPA, however, does not specify what type of information is to be held or how it is to be maintained. Thus, it is up to the schools and educational agencies to decide what information will be collected about students and how it will be secured.

There are a variety of exceptions to FERPA that allow the transfer of education records without the consent or even knowledge of the parents. For instance, unless a student's parents object, a student's contact information may be included as part of a student directory, which can then be distributed with few limitations. Additionally, education information can be released to various school or government officials, accrediting organizations, and organizations conducting research, such as studies on predictive testing, student aid programs, or instructional improvements. Further, educational institutions can release education records to school officials with a legitimate educational interest in the information. These officials, by extension, may release this information to third-party vendors who are under the "direct control" of the school officials. States, with the financial support and encouragement of the federal government, have used these latter two exceptions to develop comprehensive statewide longitudinal data systems (SLDS) to evaluate education outcomes, often with the help of private companies.

One FERPA provision in particular has attracted significant attention, namely an exception for the use of education records to audit or evaluate the effectiveness of federal- or state-supported education programs. Of concern to privacy advocates is that education records may be released under this exception to "authorized representatives" of certain federal or state government agencies (FERPA-permitted entities). Under a change of regulations made by the U.S. Department of Education in 2011, these "authorized representatives" no longer need to be persons or entities under the "direct control" of a FERPA-permitted entity. Further, they are not subject to FERPA requirements, such as allowing parents of students to review and amend erroneous records. Rather, student data controlled by these "authorized representatives" are only indirectly protected from disclosure via a requirement that FERPA-permitted entities must enter into written agreements with their "authorized representatives" to ensure FERPA compliance.

One of the privacy advocates' concerns is that it appears that not all FERPA-permitted entities are complying with these Department of Education regulations. For instance, a study by Fordham University suggests that many FERPA-permitted entities that share education records with third-party vendors have not entered into such written agreements with these vendors or that such agreements do not meet the requirements of FERPA. These concerns are exacerbated because the enforcement mechanism used to punish disclosures of education records in violation of FERPA is withdrawal of federal funds from the FERPA-permitted agency, not from the contractor. Thus, absent contracts that bind third-party vendors to the requirements of FERPA, there would appear to be no enforcement mechanisms available for unauthorized disclosures by third parties.

Congress held hearings in 2014 and 2015 on these issues. In the 114th Congress, several bills have been introduced that would amend FERPA to address these and other student privacy issues, such as S. 1322, H.R. 3157, and S. 1341. While S. 1322 would focus principally on information held by third-party vendors, H.R. 3157 and S. 1341 include more comprehensive amendments to the requirements of FERPA. All three bills, consistent with current law, would address the issue of third-party vendors indirectly by imposing requirements on recipients of federal funding. S. 1341, however, goes further, and would impose civil liability on third parties who fail to comply with the requirements imposed by the bill regarding student data.

Posted at 12/01/2016 10:30 AM