# FERPA and the Cloud: Why FERPA Desperately Needs Reform


by **Daniel Solove, TeachPrivacy**
Monday, December 10, 2012

The Family Educational Rights and Privacy Act (FERPA) is in dire need of reform. In so many ways, the statute fails to address the key issues that schools are facing. In this essay, I will address how FERPA's shortcomings impact a specific issue – cloud computing.

Cloud computing is an issue of major importance for education. Increasingly, school systems, colleges, and universities are finding it advantageous to move to cloud computing solutions for managing the extensive repositories of data they possess and the numerous information and communications services they provide.

Regarding cloud computing, FERPA fails in many ways to provide the kind of guiding hand that good regulation should provide.

## Selecting a Cloud Provider

FERPA says little about selecting a cloud provider. As I wrote in an earlier essay, there are numerous issues that schools ought to consider when choosing a cloud provider, and many terms that schools should ensure are included in an agreement with a cloud provider.

## Responsibilities of a Cloud Provider

FERPA also says little about the responsibilities of a cloud provider. The FERPA Regulations, 34 C.F.R. § 99.33(a)(1), state:

*An educational agency or institution may disclose personally identifiable information from an education record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.*

That's about all that FERPA says about the responsibilities of a cloud computing provider. FERPA says little about uses or much of anything else.

## The Responsibilities of the School Over Data

FERPA regulations state that schools must maintain "direct control" over student personal data even when outsourced to cloud computing services. According to Department of Education guidance in the 2008 regulations:

*Exercising direct control could prove more challenging in some situations than in others. Schools outsourcing information technology services, such as web-based and e-mail services, should make clear in their service agreements or contracts that the outside party may not use or allow access to personally identifiable information from education records, except in accordance with the requirements established by the educational agency or institution that discloses the information*

The problem is that this requirement is far from enough. The cloud computing provider must have meaningful policies and procedures to ensure it will follow each school's policies. The provider must have a privacy program to ensure that it will be diligent in following these policies. The school must have a way to oversee and audit compliance as well as meaningful enforcement powers. The FERPA regulations are not providing any serious protection with bite. Merely saying something in an agreement without providing for anything to ensure that it will be done seems far from exercising "direct control."

## Scope of Data Sharing Under FERPA

The scope of data sharing under FERPA is way too broad. If a school discloses education records for outsourcing its functions, the FERPA Regulations allow the school to designate the cloud computing provider as a "school official" in order to facilitate the sharing. *See* 34 C.F.R. § 99.7(a)(3)(iii). The Department of Education's model notification provides:

*A school official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted as its agent to provide a service instead of using University employees or officials (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. Department of Education, Model Notification of Rights under FERPA for Postsecondary Institutions (emphasis added).*

In many instances, schools may deem cloud computing service providers as "school officials" yet should these providers really be designated as school officials? Moreover, recently promulgated new regulations under FERPA expanded the extent to which data may be shared in order to further the Obama Administration's goal of facilitating the collection and analysis of student longitudinal data. The new regulations define two previously undefined terms in FERPA in order to expand the sharing of student personal data. FERPA permits the access of student personal data -- without consent -- to "authorized representatives" of state or federal "education programs." The new regulations expand both definitions to allow a myriad of types of third parties to access student data. Under the new regulations, educational agencies can designate "representatives" quite liberally, and this threatens to allow student data to be disseminated much more widely. Indeed, this is Department of Education's goal -- to allow for greater study of student longitudinal data.

A 2009 study by Fordham Law School's Center on Law and Information Policy found that "privacy protections for the longitudinal databases were lacking in the majority of states." Even more strongly, the study characterized the privacy protections as "weak."

Cloud computing might be a way to provider better protection for longitudinal data, but because FERPA fails to specify anything about the nature of the protections, there is no guarantee that a cloud computing provider will provide any better protections than schools or state entities. In essence, FERPA allows widespread data sharing to nearly anyone with minimal requirements.

FERPA is thus extremely vague about cloud computing. Although it has a broad scope and is very permissive in allowing data sharing to cloud computing providers, FERPA provides scant guidance and requires few limitations.

## Conclusion

Thus, FERPA fails to be effective in regulating the use of cloud computing by educational institutions. So what should school officials, parents, and politicians do?

1. In the absence of FERPA guidance, schools need to do a lot more than just follow the regulation. The law doesn't provide the kind of regulation needed, so schools need to develop best practices and adhere to them.
2. Parents should lobby Congress and their state legislatures to pass laws providing better protections of their children's data. This is an issue that should be of great concern to parents since educational institutions possess a staggering amount of personal data about students, and this data can currently be outsourced to nearly any company anywhere – even to a cloud computing provider in the most totalitarian country in the world!
3. Congress should reform FERPA. It is in dire need of reform.
4. State legislatures should get involved, and pass their own protections because FERPA is falling short.

*Daniel J. Solove is the John Marshall Harlan Research Professor of Law at George Washington University Law School, the founder of TeachPrivacy, a privacy/data security training company, and a Senior Policy Advisor at Hogan Lovells.*