Tags: Experts' Corner (/posts?filterby=Experts%27+Corner) Policy & Procurement (/posts?filterby=Policy+%26+Procurement) Education (/posts?filterby=Education)

FERPA and the Cloud: What FERPA Can Learn from HIPAA

by **Daniel Solove, (/experts/daniel-solove)TeachPrivacy**
Monday, December 17, 2012 (Monday, December 17, 2012)

In an earlier essay, I argued that the Family Educational Rights and Privacy Act (FERPA) is in dire need of reform, as demonstrated by its failure to address so many key issues regarding the use of cloud computing services by schools and educational entities.

In this essay, I will compare FERPA to HIPAA to demonstrate more reasons why FERPA fails to provide adequate guidance and limitation about cloud computing and why FERPA fails more generally as an effective privacy and security law.

FERPA vs. HIPAA: A Quick Comparison

It is an interesting exercise to compare FERPA to the Health Insurance Portability and Accountability Act (HIPAA) regulations after the HITECH Act amendments. HIPAA is far from perfect, but it leaves FERPA in the dust when it comes to the strength of its privacy and security provisions. In at least four major areas, HIPAA is far more advanced than FERPA. First, in the area of data security, the HIPAA Security Rule has detailed requirements about data security. FERPA does not. Second, HIPAA requires training of personnel about the institution's policies and procedures. FERPA does not. Third, HIPAA requires that institutions have a privacy program and a privacy officer. FERPA does not. And fourth, HIPAA (especially after the HITECH Act amendments) gives the Department of Health and Human Services (HHS) potent enforcement powers – sanctions of up to $1.5 million. HHS also has the power to audit. It has direct enforcement power not only against covered entities but also business associates such as cloud computing providers. FERPA's enforcement is narrow and virtually meaningless.

As I will explain in more depth below, these shortcomings of FERPA make it quite ineffective at dealing with some of the most important privacy and security issues facing schools. I will focus on cloud computing, as FERPA's limitations have some of the most profound effects on this issue.

Data Security

FERPA says little about data security. It doesn't provide much guidance to schools about what types of measures they should take to provide data security. Nor does it provide much in the way of requirements or guidance about what the adequate level of security should be for a cloud computing provider. And there is no requirement of having a plan in the event of a data breach.

Moreover, FERPA says little about where a cloud computing provider may store data. Indeed, under FERPA, a cloud computing provider may store data in other countries, and no criteria are provided for the adequacy of the legal privacy protections afforded in these countries. In guidance on cloud computing (http://www2.ed.gov/policy/gen/guid/ptac/pdf/cloud-computing.pdf), the Department of Education finesses the issues by recommending the following:

> *Therefore, storing sensitive education records, including medical, behavioral, assessment, and related information in special education case files, within the U.S. would be considered a best practice as it ensures that they are subject to U.S. jurisdiction.*

That's really nice, but note that it isn't a regulatory requirement, and about as binding as any advice I could give on the subject. Indeed, the entire document of Department of Education guidance, although useful, is a rather awkward document – you can almost see the Department squirm. Nearly a third of the document lays out "best practices" and advice, yet few are actually required by FERPA. If these practices are so good, then why aren't they required?

Training

FERPA has no training requirement. Policies and procedures are meaningless if people aren't trained about them. There is no requirement that cloud computing providers are trained either. Not only can a cloud computing provider fail to train employees about school policies, they can also not train about the basic requirements of FERPA.

Privacy Program

FERPA says hardly anything about the kind of privacy program schools must have or require any internal assessment. There is no requirement that a school have a privacy officer – or no such requirement for any entity providing cloud computing services. That means that there need not be anyone in charge of privacy – nobody who is responsible for the data, nobody to call if there's a question or problem.

Enforcement

FERPA's enforcement leaves a lot to be desired. FERPA's enforcement is quite minimal, lacking a private right of action and having a sanction so implausible it has never been imposed in the 35+ year history of the law. That sanction is a withdrawal of all federal funds. It will never happen. So many steps must occur between the violation and the ultimate sanction being imposed that a school would literally have to walk a plank that would stretch halfway across the Atlantic Ocean. A school must be beyond bad in a systematic way to be even close to having the sanction imposed – and probably then it will still fail.

The Department of Education only has power over the schools and education agencies it funds. Cloud computing providers are not directly subject to this enforcement power. In some circumstances, they can be restricted from contracting with schools. But the vast bulk of the Department's enforcement is on the schools themselves, and that enforcement is virtually meaningless.

Conclusion

When it was passed, FERPA was ahead of its time, but now it has fallen way behind. As I have demonstrated with the example of cloud computing, FERPA is not providing the kind of guidance and regulatory parameters that are most needed. Comparing FERPA to HIPAA starkly demonstrates that FERPA is missing so many key elements of modern privacy regulation that it is need of a major overhaul.

In light of the current state of FERPA, what should be done? Here is some advice for parents, politicians, and schools:

1. Parents need to look at what their schools are doing about student privacy and speak up, because the law isn't protecting their children's privacy.
2. School officials who want to develop a more meaningful and robust protection of privacy should talk to government officials who are tasked with complying with HIPAA. They can learn a lot from studying HIPAA and following some of its requirements.
3. Congress should remake FERPA more in the model of HIPAA. If Congress won't act, state legislatures should pass better education privacy laws.
4. Because FERPA does not provide adequate oversight and enforcement of cloud computing providers, schools must be especially aggressive and assume the responsibility. Otherwise, their students' data will not be adequately protected. School officials shouldn't assume that the law is providing regulation of cloud computing providers and that they need not worry. The law isn't, so right now the schools need to be especially vigilant.

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

More information

Permalink (/2012/12/17/ferpa-and-the-cloud-what-ferpa-can-learn-from-hipaa) .

Post a comment