Insight

Student Data Privacy: 5 Rules to Follow

CHAD MILLER, WILL RINEHART | JUNE 4, 2015

Introduction

Beginning around 1983, IBM Clones (PCs), namely the Apple II, began showing up in public schools across the nation, and with these PCs came the proliferation of educational software such as *The Oregon Trail* and *Where in the World is Carmen Sandiego.* Within three years nearly 25 percent of all public schools had student access PCs. Fast forward to today, and nearly all schools provide students access to technology ranging from desktops to tablets. These devices are used for tasks such as direct instruction, drill and practice, remediation, college counseling, and student assessment. Through the use of the new technology, developers were introduced to the benefits of collecting student level data. Over the last 30 years the education technology sector honed its skills and now has the ability to collect huge amounts of user data. And while student data is an important resource for teachers and parents creating personalized, more effective instructions for their students, as Digital Learning Now states, it is also vital that parents and students can trust that their child's information is secure and used correctly.

Over the last few years policymakers have taken notice of the privacy advocate's outcry for revising or modernizing student data policies. As proof, consider that in 2014, 37 states introduced 110 student data privacy bills, 28 of which were eventually signed into laws in 20 states[1]. Recently, Congress began keying in on the issue, hoping it offers a chance for both sides of the aisle to demonstrate their ability to work together by updating federal laws dealing with student privacy, such as the Family Educational Rights and Privacy Act (FERPA).

FERPA

Family Educational Rights and Privacy Act of 1974 is a federal law that ensures parental rights and privacy with student records. All educational institutions that receive federal funding must comply with FERPA, and elementary and secondary schools must inform parents of their rights under FERPA every year. FERPA includes four main rights:

1. *The right to control disclosure of education record*

Schools have the right to supply information such as student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must also give parents an adequate amount of time to disallow the disclosure of this information.

2. *The right to review education record*

Parents or eligible students have the right to request an education record. School officials must supply the

education record within a forty-five day period. An education record includes, but is not limited to, grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files.

3. *The right to request amendment of inaccurate or misleading portions of education record*

FERPA only requires consideration of requests to amend information that is inaccurately recorded. Requests for amendments such as a grade change, removal of evaluations, or removal of disciplinary actions are not covered under the FERPA amendment proceeding.

4. *The right to file a complaint regarding non-compliance of FERPA with the Department of Education (ED)*

The Family Policy Compliance Office investigates complaints. In order to be investigated, complainants must file their complaint within 180 days of the incident. The investigation is closed once agreement between both parties is reached.

Updating Policies

With four different student privacy bills being considered, Congress must decide which, if any, they will pass. The education technology industry is quickly moving to create new tools and discover means of monetizing that content. In response, policymakers are now trying to determine what kinds of regulations are necessary to protect students. The natural drive is to overprotect students and children, and rightly so, but research from diverse fields and countless real life examples prove that perception of risk is subjectively biased. Instead of being bogged down by trying to prevent any and all mischief, sound policy demands that any new bill be narrowly tailored to specific and cognizable harms.

A number of affected parties in the education sector have collaborated to establish generally accepted principles for safeguarding student data, and from these principles, a set of recommendations that congressional policymakers should adhere to can be formulated.

Know "what data"

At a minimum, annual audits should be publically published detailing what student data is currently being collected and how that data is being stored. Requests for additional data should also be published and supported with a needs analysis.

Continue Parent Access

As FERPA currently calls for, parents should have the right to obtain the data being collected as well as the right to request correction. As an update, changes to FERPA should be made that require the disclosure of all parties that are collecting or have access to student data. There should also be an appeals process for parents who wish to block some or all 3rd party access to their student's data.

Only Collect Data Beneficial to Student Achievement

Religious, political, or other affiliations not related to existing subgroups used in disaggregating educational data and or are otherwise not beneficial to education outcomes should not be collected.

Restrict Advertising and Selling of Data to 3rd Party Providers

When polled roughly 64 percent find targeted advertising to be invasive; however, about 20 percent of those surveyed want the benefits of targeted advertising. Still, the public generally thinks advertisers should be regulated more stringently. On the other hand, the selling of data to third parties seems to violate an implicit contract between the student and the school system. More often than not the student and the school system have common goals and outcomes that do not always align with third party vendors.

Establish a Culture of Privacy

Some have criticized the current piecemeal approach in US privacy protection as being fractured and are using debates like this one to push for overly broad privacy protections. In fact, the US is home to a robust privacy culture and Chief Privacy Officers (CPO) are common across industries. The International Association of Privacy Professionals now boasts over 20,000 members, nearly double that of 2012, with most of the members residing in the US. This year alone, privacy spending by the Fortune 1000 will approach $3 billion. More than just passing a law where compliance becomes the goal, Congress should take a page from industry and foster a culture within all levels of the educational system where privacy is of utmost importance.

Cost of Regulating

As well intentioned as any legislation might be for students, real costs come with changes in policies. According to a previous AAF study, the ED's regulatory burden already exceeds $3 billion annually, and it is known that privacy regulations have costs as well. Take, for example, another major piece of privacy legislation, the Children's Online Privacy and Protection Act (COPPA). In a review of the law, the Federal Trade Commission (FTC) estimated that the annual compliance costs for current web services were $6,223, while new services had to pay $18,670[2]. As some have argued, this is a cost worth bearing. On the other hand, the costs crystallize the current industries players and raise the price of entry, thus making disruption all that more difficult. Education costs are rising at all levels, which privacy regulations are sure to compound.

Much of the education technology that will be subject to new regulations employ predictive algorithms, which can help steer kids toward more targeted interventions. Educators benefit as well, since they can be informed of specific places that need improvement. Importantly, the reforms being discussed and the recommendations here do not restrict operators from sharing aggregated de-identified student data for research and development purposes, and nor should it. The potential for better educational outcomes is very real and should be encouraged.

Conclusion

On balance, what Congress should strive for are targeted policies that recognize the benefit to student achievement education technology has grown to provide. Going overboard with privacy regulation could mean that students don't get the kinds of tools that they need to succeed. More likely, however, is that an onerous bill will add more to the burgeoning cost of education.

[1] STUDENT DATA PRIVACY: BUILDING A TRUSTED ENVIRONMENT http://excelined.org/data-privacy/