FOSI Briefs

Family Online Safety Institute

July 17, 2014

Student Data Privacy: The Challenges and Opportunities

With the introduction of over 100 state bills, draft federal legislation, recently released industry released best practices and updated Department of Education guidelines in 2014 alone, student data privacy is an increasingly important issue across the United States.

Congressional hearings, media stories, and ongoing public debate have furthered the discussion and divided general opinion. At the extremes there are those who advocate for abundant use of technology both in the classroom and throughout the education system, highlighting the many advantages of data driven learning. In opposition, are people who express concern about the hazards of collecting and storing the personal information of children. In the middle there are those searching for the balance between allowing children to access all the benefits of data based-learning, while ensuring that private information remains protected.

There has been misinformation and misunderstandings about the uses of student data, as well as the state of current and proposed regulation designed to protect this highly sensitive information. Drawing from our recent panel discussion on Capitol Hill, and through this brief, FOSI's intent is to give clarity to an incredibly important topic that could revolutionize education.

Bus routes, student lunch allocations, group projects, attendance tracking, online testing, parental access to assessment results - these are just some of the thousands of ways that student data is used today. The technologies that are currently on offer allow teachers to set online tasks for children in and out of the classroom. They provide children with email so that they can communicate with each other, not to mention the incredible amount of information and guidance that the tracking of student performance can give educators. Students who have learning difficulties can have their individualized education plans follow them through school, and parents can access their children's grades in real time.

All of these practices demonstrate the tremendous benefits of education technology; possibilities of data driven learning are immense. However, in order to fully realize the potential of these new resources, teachers and administrators must be educated on how best to use them. Even more importantly, parents must remain informed of the uses of the data and the personal information itself must be protected and managed in a way that means that it can benefit children and not be used to their detriment.

Concerns about student data collection have been raised by a large cross-section of society, from policymakers to parents, and educators to privacy advocates. Fears have focused mainly on the amount of information being collected and the motives behind it, in addition to the uses and storage of students' personal information. Parents have been particularly upset at the lack of information provided to them about wider data sharing practices. But by far the most concern expressed has been around the sharing of this highly confidential data with private organizations and companies outside the school administration.

Outrage from parents' groups contributed to the demise of inBloom, the organization established with the support of the Bill and Melinda Gates foundation, with the aim of "tailoring education to students' individual learning needs." News articles on the practice of scanning students' email by Google, through Google Apps for Education, led to a company change of policy. The concept of direct marketing to children, resulting from the collection of information (for example, a child taking a math quiz online and then being contacted with a book to improve their

understanding of questions that were incorrect), has caused concern. Also causing unease is the perceived inability to make changes to the information, and the fact that it follows a child throughout their school career. Should a school suspension in 5th grade still be relevant in 12th grade? Many feel this is not an acceptable retention of data for young people, not to mention the ongoing anxiety about the potential for data breaches and information falling into the wrong hands.

The US states have been quick to act, seizing on a perceived void in federal regulation to pass laws designed to protect children in their state. Currently, educational data collection and storage in the US is regulated at a federal level. Relevant legislation includes the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA) and the Protection of Pupil Rights Amendment. However, as use of technology in the classroom and in school administration expands, there are increasing calls, from privacy advocates to parents, for more robust protection.

FERPA requires that personally identifiable information that is shared with service providers be limited to uses otherwise performed by the school's own employees. The provider must be under direct control of the school, and the information shared can only be used for educational purposes. The Department of Education issued further guidance in February 2014 in order to, "help school systems and educators interpret and understand the major laws and best practices protecting student privacy while using online educational services."

COPPA also regulates student data collection and requires consent to share the information of a child under 13; the Protection of Pupil Rights Amendment requires parental notice and possible opt-out of activities involving the use of students' personal information for marketing and advertising purposes unrelated to the education purpose for which it was collected. Furthermore, all data sharing beyond the school is regulated by contracts, entered into by both parties, which bind the service providers to certain terms, including those related to use and storage of data.

Recent state proposals have ranged from those prohibiting the sharing of personal data without parental consent to those that outlaw the collection of certain types of data from students' altogether. Many have focused on the prohibition of marketing to students based on information collected from sensitive data.

At a federal level, Senators Markey and Hatch released a discussion draft in May 2014 that proposes the implementation of safeguards to protect student data and ban marketing to students. It also provides a right of access for parents to the information held and minimizes all data collection. In a recent report from the White House entitled, 'Big Data: Seizing Opportunities, Preserving Values,' the Obama administration stated that, "students and their families need robust protection against current and emerging harms, but they also deserve access to the learning advancements enabled by technology that promise to empower all students to reach their full potential."

Clearly there is a desire to protect student information, but at the same time hopefully there is an acknowledgement that the considerable benefits of this technology must be maintained and ensured. Data evangelists and those who argue for the benefits of educational data usage have been dismayed at certain inflammatory news reports and state laws, claiming they will at best chill the creation of resources for education and at worst ban the collection of essential student data completely. Many recognize the risk of creating a technological mandate that quickly becomes outdated and ultimately stifles innovation.

The ultimate solution to this problem is a shared responsibility. Parents must be engaged in their children's learning, be given all the information and have the opportunity to consent to data usage. Schools must learn how to use the data effectively and how to protect it. Companies must uphold their end of the bargain and limit marketing to students as well as ensuring all data is highly protected. And school districts should nominate a privacy officer, to take a leadership role and assist schools in negotiating contracts, complying with existing law and protecting data.

There is no doubt that student data collection, use and storage is an intensely emotional subject, but ultimately the debate must deal with specifics rather than hypotheticals. There is great potential for student empowerment and achievement, realized through informed and engaged parents, and educators taught to use resources to the best of their ability. Fear of data and how it can be misused should not prevent us from meeting the promise of technology.

There is nothing more important than the protection of children's data, but we must ensure that the techniques devised do not unnecessarily impede the use of today or tomorrow's technology. On student data, we must not relinquish the opportunities in the face of the challenges.

Emma Morris
International Policy Manager
emorris@fosi.org

About FOSI

The Family Online Safety Institute is an international, non-profit organization which works to make the online world safer for kids and their families. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.