Supporting Parental Choice for Student Data

Jules Polonetsky and Brenda Leong
Future of Privacy Forum
September 2016

Students from American middle schools can take 3-D guided virtual tours of the Louvre, and practicing their French with questions to the tour on-site museum curator, without ever holding a bake sale. High schoolers researching the American Revolution can look up the actual newspaper articles published in the Boston Globe in the 1770s. Any school, no matter how isolated, can offer Russian or Chinese language lessons, or sponsor their gifted youngsters into a nationwide community to participate in conversations, contests for physics, biology, or art. These possibilities and many more are the result of integrating educational apps, mobile devices, and educational products and services into classrooms and school labs.

Technology utilized by an effective teacher helps every student learn to the best of their ability, by taking advantage of opportunities not previously available. In schools using technology well, this is a complementary process that engages students with techniques and tools they use outside of school, while also expanding their understanding via new applications of the technology. Teachers use online textbooks and worksheets, website content and video programs; games (that might really be a short quiz on the information just covered); or shared documents or chat rooms for small groups of students to meet and collaborate. The teacher can see what each student has done, and when the work was completed – perhaps intervening with a private comment or encouragement to the group, when he sees the right moment. A class project might allow the student to tie in photos, researched information, and her own text into a final presentation, which is then uploaded for the teacher's review and grade. Students can continue the learning process outside of the classroom, working easily from home or wherever they have an Internet connection. Ideally, teachers can also use educational resources to tailor

lesson plans for individual students and provide a personalized learning experience based on academic ability or special needs.

Many of these opportunities rely on vendors contracted by schools to provide technology and software programs and services. From global companies, to digital divisions of traditional textbooks, to teachers launching their own apps, a wide range of companies may be responsible for safeguarding student data. Most of these companies take their responsibilities seriously, but concerns have often been raised about the practices of companies large and small.

Policymakers have responded to those concerns about how vendors handle student information by proposing new state and federal legislation. One response to these challenges is the Student Privacy Pledge ("Pledge"). Launched in 2014, the Pledge is an express, public commitment to responsible data use that now has more than 300 ed tech company signatories – from the education market leaders to the smallest start-ups.[1] A legally enforceable policy statement, the Pledge details these companies' commitment not to sell, misuse, or unfairly benefit from student data, but to use it on behalf of the school in support of the educational purpose for which it was created.

State legislatures have also responded to student privacy concerns. In 2015, there were over 180 student privacy bills[2] under consideration in 46 states, up from the previous year record of 110 student privacy bills proposed in 36 states. In 2016, another 17 laws were passed in 16 states. In addition, in 2015, the U.S. House of Representatives[3] and U.S. Senate[4] each proposed legislation directed at ed tech

[1] Student Privacy Pledge. Future of Privacy Forum, www.studentprivacypledge.org.
[2] Data Quality Campaign. "Student Data Privacy Legislation: What Happened in 2015, What Is Next?" http://dataqualitycampaign.org/wp-content/uploads/2016/03/DQC-Student-Data-Laws-2015-Sept23.pdf.
[3] "Messer, Polis Introduce Landmark Bill to Protect Student Data Privacy." http://polis.house.gov/news/documentsingle.aspx?DocumentID=397810.
[4] S.1788 - 114th Congress: SAFE KIDS Act. Text. https://www.congress.gov/bill/114th-congress/senate-bill/1788/text

vendors as well as drafting rewrites or proposed amendments to the Family Educational Rights and Privacy Act (FERPA) to update the responsibilities of schools and educational agencies.[5]

California was an early leader in passing a student privacy law, known as SOPIPA. SOPIPA is proving to be effective in helping guide companies to comply with student privacy requirements. But in one important area, the law falls short and is a barrier for parents who want to make sure their children can take advantage of opportunities which may be available to them. If the parent of a student using a school service sees an opportunity for their child that has not been contracted for by their school, SOPIPA bars the parent from enabling that option.

For example, parents may want to make their child's data available to a tutoring program, to a college mentoring program, or other educational support services. They may want a child's art or photos shared in a competition sponsored by an outside organization. They may seek to connect their child's project, report, or performance to an extracurricular debate or model United Nations club, Boys and Girls Clubs, math camp, travel programs, or computer science training. They may just want to be able to highlight their child's achievements for internship and volunteer opportunities, where showing more "whole-person" data can provide a better picture than a one-time, high stakes SAT score. Other parents may want to use their child's record in affiliation with school programs or organizations through which they homeschool their child.

For those bills with overly restrictive language, parents face a significant barrier for a wide range of uses of data they may want to enable. With all the extracurricular and specialized opportunities available online, there are an increasing number of areas where parents may want to use school-related data from or about their child to support activities outside of the school's curricular programs.

[5] H.R.3157 - 114th Congress: Student Privacy Protection Act." https://www.congress.gov/bill/114th-congress/house-bill/3157/text?resultIndex=1.

This limitation is particularly relevant for children with disabilities or learning challenges who are some of the active users of multiple resources outside the school. Transitioning to new or added services without the ability to easily integrate existing digital information creates a tremendous burden on these parents when each new program may have to reassess and freshly establish or document the child's abilities and requirements.

Some state bills do provide limited exemptions for parent to request to send data to colleges or for employment or to seek scholarships and financial aid, but all other options are banned. Other states recognized the broader need for parental control and passed legislation that allows a parent to tell a vendor to send their student's data to programs or options they expressly choose.

Certainly, there may be some schools that do not want to enable parents to approve additional services. They might worry about parents being asked to pay a fee unnecessarily, or about parents making poor decisions to share data with outside vendors in ways that allow marketing or individual profiling. These are valid concerns that should inform the conversation at the local level, where parents and school communities can decide together on the best options for their students. For example, legislation could ensure data is shared only for education-related purposes and only with very specific and clear consent from parents. This model is the path taken by the ACLU, in its new student privacy campaign[6] to advance protections across the US, and was also included in a number of earlier state bills, some of which have become law.

A parent's authority to advocate for their child should not be limited to certain recipients, and should certainly not be banned entirely. Any student privacy law should allow schools and parents to consider these decisions and create local policy together, instead of imposing a blanket ban on parental choice. Because even the most detailed statute could never anticipate all the things a family might

[6] ACLU Student Information Systems Model Legislation. https://www.aclu.org/legal-document/student-information-systems-student-data-privacy-model-legislation.

choose, laws should simply be written with an exception that allows parents the responsible choice for the further disclosures they feel are in the best interest of their children.

Those who oppose this full control being left with parents are concerned that a parent's consent is not always adequately informed; that parents may not realize or understand everything they've been asked to share, to whom the data will be sent, or all the purposes the data can be used for. Anyone who has quickly clicked through an "I agree" page for an app or online service understands this is a valid concern. However, the right solution is not to completely prohibit parental consent and make it illegal, but simply to make it rigorous and informed, and to ensure any data shared will only be used for authorized purposes.

Parents remain the best judge of what opportunities should be available to their children. When they wish to seize those opportunities, any release they sign must be clearly written and expressly authorized, limited only to the purpose they intend. Perhaps the release should occur only if parents are the ones who initiate the request (no "default offers" made available to everyone); or acceptance could require multiple inputs from the parents to confirm their understanding; or school policies could mandate an explicit direct request/response exchange between parent and vendor before the disclosure is allowed.

Setting a high bar for informed consent is reasonable, but completely taking away a parent's right to release the student information actually impedes freedom of choice by the person most closely in touch with their child's best interests. Some states that have wisely recognized this point by including clear exceptions for the explicit requests of schools and parents have taken a path that better reflects today's rapidly changing learning environment.[7]

[7] In Maryland, for example, state legislators provided options for parents who expressly approve new uses of student data. General Assembly of Maryland: "Student Data Privacy Act of 2015." http://mgaleg.maryland.gov/WEBMGA/frmMain.aspx?pid=billpage&tab=subject3&id=hb0298&stab=01&ys=2015RS

Neither legislators, nor schools, nor even parents can anticipate all the potential options becoming available to aid in understanding and managing their child's education. Certainly we should not expect lawmakers or schools to specify the full range of possibilities. Instead, the optimum policy defers to parents to determine when and how to share data about their own child. Parents understand that technology continuously plays a role in their child's development and educational success. We should trust them – in partnership with schools – to make smart decisions. Ultimately, legislation designed to help students must empower parents and provide them with clear options to further use their child's educational data as they see fit.

Parents, educators, and policymakers share the important concerns about the responsible use of student data. They want students to have the best possible educational opportunities, to be protected, and to know that the educational system is robust and effective. Laws that restrict that right are putting fears of the unknown ahead of real opportunities for schools and families to partner to ensure the progress of students. Parents, as those most in-tune with their individual child's needs, have the right to be an active partner and the final decision about additional sharing and use of their child's information.