Learning from Student Data

The debate about the safety of student data arose quickly, and there are good ways to address parent concerns. Opting out of data collection is not one of them.

by Kobie Pruitt

Just as adults' personal lives and data increasingly inhabiting online spaces, so are students. While this shift brings many benefits and the possibility of learning tailored to individual students' needs, it is also brings new challenges. Students create an electronic trail of information that creates an obvious concern: How can they enjoy the better learning outcomes technology makes possible but still maintain control of their data and be protected?

Nearly two years ago, a debate ignited over student information from multiple states and regions being collectively stored with the data repository InBloom. Critics charged that the not-for-profit service provider could potentially sell, misuse, or otherwise put at risk student data it held for schools. Surprised by the backlash, InBloom was ill prepared to explain its services to parents. Critics didn't trust a third party whose name they didn't recognize and who didn't provide any service they could see, or track to a direct benefit for their child's educational experience.

InBloom looked to school leaders, who were relying on the vendor to support school data handling, analysis, and reporting, to tell parents that nothing had changed. Other ed tech vendors already were managing student data, often storing it with cloud providers rather than keeping it on local servers. Apps and other programs collected student data as they provided educational services. InBloom would join the ranks of outside companies helping schools manage data better.

But school leaders did not have ready answers for the critics. For a small but determined group, InBloom became a target for larger concerns about education reforms generally, in particular questions about curriculum reform or and standardized testing. The fact that InBloom's charitable backers included foundations associated with some of those reforms only served to conflate student data privacy with other hot-button issues.

The resulting pressure found school leaders without clear answers specific to student data privacy concerns. The primary federal law, the Family Educational Rights and Privacy Act (FERPA), enacted decades earlier, was frequently dismissed as out of date.[1] In actuality, however, the US Department of Education has regularly updated regulations under the law multiple times to take into account new technologies and issues. Even so, FERPA regulated schools, not vendors, so concerns were raised that it did not effectively bar companies from misusing education data.

In 2014, legislators in 36 states responded to these concerns by introducing 110 bills related to student data privacy.[2] By the end of 2014, 21 states had passed 24 new student data privacy laws. The following year saw a dramatic increase, with 47 states introducing 188 bills addressing student data privacy. Five months after InBloom closed its doors, California passed the Student Online Personal Information Protection Act (SOPIPA), which put vendor restrictions in place.[3] Twenty-six

Box 1. FIPPS

To understand privacy rights and privacy laws and apply them to student data, it is important to start with the Fair Information Practice Principles (FIPPs), a set of basic rules agreed to by most of the democratic countries in the world, which form the basis of most privacy laws in the United States.[a] Among other things, the FIPPs require data collectors to specify the purpose for which they are collecting data and to seek informed consent for its collection and use. Additional permissions are needed only when the use is unrelated to the initial, primary purpose.

What's the primary purpose of collecting data in schools? Some "primary use" categories for student data collection are obvious. Schools cannot function without basic information about students and parents. They need to record grades, know who is eligible for subsidized lunches, and who has special learning needs. Schools need to share data with vendors who operate cafeterias, school buses, or more recently, data storage systems for the school. In general, administrative and educational purposes are primary purposes of a school system, and thus data collection is necessary and expected.

In recent decades, the quantity of student data collected has steadily increased, and it has been combined and stored and analyzed in every larger data sets for increasing levels of analysis.

[a]Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," (n.d.), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

other states subsequently used SOPIPA's framework in their own student privacy legislation (for more on SOPIPA, see Amelia Vance's article elsewhere in this issue).

During the same period, education service providers began to take a more public stand to show their support of responsible practices for handling student data. In order to help them build public trust, the Future of Privacy Forum and the Software and Information Industry Association began coordinating with these companies to sign a Student Privacy Pledge. Pledge signers committed to not sell student data, to use data only for purposes that schools authorize, and to refrain from behavioral advertising, among other restrictions. The pledge is a legally binding commitment for the vendors that sign it, enforceable by the Federal Trade Commission and states' attorneys general. To date, over 230 companies have signed on and the White House has endorsed the pledge and urged every vendor handling student data to make the commitment.

But at the end of the day, there is only so much that vendors, state laws, pledges, or the US Department of Education can do to explain to parents how and why student data are collected and what protections are in place. Those who are trusted with students and their data need to be able to articulate the reasons for data collection and how it benefits students and teaching. When these reasons are not clear, parents question the process and are suspicious of the risks they see, and may begin to question the right of the school or district to collect and hold data about their children.

Between consumers or parties to agreements in other contexts, the exchange of data for a service is a voluntary transaction, and in many cases there are levels of control for what data are provided. In some cases, there is the offer to "opt in" with more information for additional services, or "opt out" for collection or use of data that the user may feel is beyond the scope they are willing to provide. Because of this mindset, some concerned parents have sought these same controls in the student data context — the change to opt in to various school programs or services, or opt out of others. For the most part, however, these are not viable strategies within the primary role of the educational system, and it is important that parents understand the distinction, as well as the limited context in which such controls can be applied.

The collection of student data within the educational system is not a discretionary exchange. In addition to the direct individual record created on each student based on their academic performance within their current classroom or grade level, there is data use to understand how well students perform over time, how well a school system is serving different populations, and how well different educational strategies are succeeding.

At the individual level, processes in a public educational system must be safe and sufficient for all students. If a particular program or activity results in a situation that carries unacceptable risk such that opting out is required, then it is not a program that should be used in the first place. Just as a student cannot "opt out" of being

marked for attendance or for being graded, the process that collects and records grades and attendance must be sufficient for the protection of all the students' grades.

Beyond the individual level, there is likewise no justification for allowing individual families the opportunity to withhold their particular records from the aggregated uses of student data. The metrics for how classes, schools, or districts perform must be reliable and accurate. If primarily low-income or, perhaps, high-income students were to opt out, schools and policymakers would be misled as to the real results of the educational system, lacking information that accurately reflects all sectors of the school community.

There are, however, some secondary uses of data where parents can and should make choices, namely, in contexts where any sharing of student data is for purposes unrelated to primary educational activities. Yearbooks, extracurricular activities, or other programs outside the direct educational process are all situations where parents should have the option of how far to participate. In fact, these are the areas where federal law mandates that schools give parents the chance to opt out.

Concerns of frustrated parents over policies they oppose need to be heard and resolved. They should certainly be provided assurances that their children are safe. But their concerns need to be addressed by fixing problems for all students, as part of an educational system that is appropriate for everyone. If a chosen online service or application is too risky, then school leaders must choose a different service provider or refrain from using it.

Policymakers seeking to address parent concern by crafting privacy rules for student data need to consider the full scope of data collection and use to sustain the value of education, and particularly look to avoid the unintended consequences of restrictions written too broadly. Fear should not be the basis of policy development or be allowed to hold back genuine improvements to the educational system.

School leaders, working in partnership with ed tech vendors, owe parents a clear understanding of how and why data are collected and used. A national survey conducted by the Future of Privacy Forum showed that parents support technology in the classroom and the collection and analysis of student data when they understand the benefits for their child and her class or school.[4]

School leaders must be ready to answer questions by taking advantage of the many resources available. Additionally, if staff at state and local education agencies, and even policymakers and legislators, familiarize themselves with these resources, they will all be better able to help parents understand how schools and states are using data to benefit students and provide better learning outcomes. ■

Resources

Department of Education PTAC
http://ptac.ed.gov/

FERPA|Sherpa
http://ferpasherpa.org/

Student Privacy Pledge
http://studentprivacypledge.org

CoSN Trust Framework
http://www.cosn.org/Framework

iKeepSafe, FERPA Assessment
http://ikeepsafe.org/privacy/ferpa/

iKeepSafe, California Student Privacy Badge
http://ikeepsafe.org/privacy/california/

Data Quality Campaign, "Roadmap to Safeguarding Student Data,"
http://dataqualitycampaign.org/find-resources/roadmap-to-safeguarding-student-data/

Common Sense Media
https://www.commonsensemedia.org/privacy-and-internet-safety

Amelia Vance, "Trends in State Legislation on Student Data Privacy," *Policy Update* 22, no. 4 (Alexandria, VA: National Association of State Boards of Education, 2015) http://www.nasbe.org/wp-content/uploads/NASBE-Policy-Update-2015-Legislative-Session-Data-Privacy_-June-2015.pdf.

[1]20 U.S. Code § 1232g — Family Educational Rights and Privacy Act, https://www.law.cornell.edu/uscode/text/20/1232g.
[2]Student Data Privacy Legislation: What Happened in 2015, and What Is Next?" (n.d.): n. pag. Data Quality Campaign, http://dataqualitycampaign.org/wp-content/uploads/2015/09/DQC-Student-Data-Laws-2015-Sept23.pdf.
[3]Student Online Personal Information Protection Act, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177.
[4]Beyond the Fear Factor: Parental Support for Technology and Data Use in Schools." (n.d.): n. pag. Future of Privacy Forum, https://fpf.org/wp-content/uploads/2015/11/Beyond-the-Fear-Factor_Sept2015.pdf.

Kobie Pruitt is education policy manager at the Future of Privacy Forum. kpruitt@fpf.org