STUDENT DATA:
TRUST, TRANSPARENCY, AND THE ROLE OF CONSENT

OCTOBER 2014

JULES POLONETSKY
EXECUTIVE DIRECTOR

JOSEPH JEROME
POLICY COUNSEL

FPF
FUTURE OF PRIVACY FORUM

STUDENT DATA: TRUST, TRANSPARENCY AND THE ROLE OF CONSENT

JULES POLONETSKY
EXECUTIVE DIRECTOR, FUTURE OF PRIVACY FORUM
JOSEPH JEROME
POLICY COUNSEL, FUTURE OF PRIVACY FORUM

OCTOBER 2014

CONTENTS

FPF

INTRODUCTION

Over the past decade, new technologies in schools have generated an "explosion of data" for public school systems to use and analyze.[1] According to Secretary of Education Arne Duncan, student data holds the promise of providing educators with a roadmap to reform: "[Data] tells us where we are, where we need to go, and who is most at risk."[2] The Department of Education has identified using student data systems to help students and improve education as a top national priority.[3]

At the same time, the increased focus on data has raised legitimate privacy questions. Parents are worried that student data is being used for marketing purposes while studies suggest that student data may be being shared without appropriate contractual and legal safeguards.[4] There is as yet no consensus among school districts as to how best to tackle data-privacy concerns.[5] Legislators seeking to respond to these concerns have proposed laws aimed at enabling parents to opt-in or opt-out of various data practices at their children's schools. On the surface, a "notice and choice" regime has an intuitive appeal: "Just ask parents, and if they say 'no,' don't collect the data!" But upon further reflection, this only raises additional challenges.

Providing parents with more notice and choice may do little to actually protect student privacy. As the President's Council of Advisors on Science and Technology recently remarked, "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[6] Worse, if parents are unable or unwilling to parse out complex

---

1 *By the Numbers - How Data Use Is Transforming the Classroom*, Education Northwest (Spring/Summer 2011), http://educationnorthwest.org/resource/1642.

2 Arne Duncan, U.S. Sec. of Ed, Robust Data Gives Us the Roadmap to Reform, Address at the Fourth Annual IES Research Conference (June 8, 2009), http://www2.ed.gov/news/speeches/2009/06/06082009.html.

3 U.S. Dep't of Ed., Use of Education Data at the Local Level: From Accountability to Instructional Improvement (2010), http://www2.ed.gov/rschstat/eval/tech/use-of-education-data/use-of-education-data.pdf.

4 Common Sense Media, *National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared* (Jan. 22, 2014), https://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern; Natasha Singer, *Schools Use Web Tools, and Data Is Seen at Risk*, N.Y. Times (Dec. 12, 2013), http://www.nytimes.com/2013/12/13/education/schools-use-web-tools-and-data-is-seen-at-risk.html.

5 Julia Freeland & Alex Hernandez, Clayton Christensen Institute, Schools and Software: What's Now and What's Next? 28 (2014), http://www.christenseninstitute.org/wp-content/uploads/2014/06/Schools-and-Software.pdf.

6 President's Council of Advisors on Sci. and Tech., Exec. Office of the President, Report to the President: Big Data and Privacy: A Technological Perspective xi (May 2014),

data policy statements, they could end up unintentionally excluding their children from critical services necessary for their education. Instead of relying on rote opt-in and out tools, we need to think about *better* ways to inform parents about how their school children's data is being used, and to provide students and parents with better tools to inform learning.

Proposals to limit the accessibility of materials, the deployment of education technologies, and the use of data analysis in schools could have the unintended consequences of leaving some students behind and crippling school administration. Proposed legislation in New York, for example, would have made it almost impossible – and far more expensive – to manage schools on a day-to-day basis. According to State Education Commissioner John King, "[e]verything from course scheduling to transportation to school lunches to high school transcripts for college applications would be impacted."[7]

Like many other organizations,[8] schools partner extensively with outside parties, including volunteers and contractors, to perform basic administrative tasks. Schools use outside parties to run cafeterias, administer electronic student information systems and provide digital learning resources, and these relationships often require sharing student information. Privacy laws generally recognize that these third parties who act on behalf of an organization should be treated as an integral part of the organization itself, so long as the organization remains in control of the data. Thus, efforts to encourage parents to opt-out of school systems simply because certain functions are outsourced could be especially disruptive.

This paper discusses how data is used both in classrooms and by educators and policymakers to assess educational outcomes.[9] It addresses the practical implications of consent requirements both for day-to-day school management and for the education system as a whole. It explores how existing federal laws,

---

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

7 Andrew Ujifusa, *Student-Privacy Protection Focus of New York State Legislation*, EdWeek (June 17, 2013), http://blogs.edweek.org/edweek/state_edwatch/2013/06/student-privacy_protection_focus_of_new_york_state_legislation.html.

8 *Managing Data Security and Privacy Risk of Third-party Vendors*, Grant Thornton (2011), http://www.grantthornton.com/staticfiles/GTCom/Health%20care%20organizations/HC%20-%20managing%20data%20-%20FINAL.pdf.

9 Because schools can generate a wide variety of data, we recognize that there are different understandings of what properly constitutes "student data" and that some of this information may go beyond what federal privacy laws cover or how student's personally identifiable information (PII) is defined. While businesses and advocates broadly agree that protections are necessary for PII collected in the course of schooling, debate exists around under the sensitivity of metadata or various forms of aggregated or de-identified information. When we use student data in the context of this paper, we mean data captured by FERPA education records as well as other potential PII where general consensus suggests additional protection is needed.

including the Federal Educational Rights and Privacy Act (FERPA), protect student data. It reviews the activities of vendors and the role of individual consent in data processing by the health and financial sectors. It proposes that in lieu of focusing on the technicalities of parental consent requirements, legitimate privacy concerns must be addressed in a manner that protects all students. It argues that parents should never have to opt-out of embracing new technologies simply in order to protect their children's privacy. Instead, to foster an environment of trust, schools and their education partners must offer more insight into how data is being used. With more information and better access to their own data, parents and students will be better equipped to make informed decisions about their education choices.

USES OF DATA IN SCHOOLS

Education systems have always relied on student information to effectively administer schools and improve classroom learning. Schools track student attendance and test scores in order to assess their performance; guidance counselors use report cards and disciplinary records to ensure students are on track; student data is used to administer free or reduced lunch programs, manage bus schedules, and accommodate students with various disabilities. These data uses are neither new nor controversial.

What has changed radically over the past few years is the development of new technologies that allow schools to better manage, analyze, and use their information. The debate surrounding this seismic shift in technological data management capabilities has often been conflated with broader educational policy discussions around issues such as the Common Core Standards and assessment of teacher and school performance across districts and states. While these broader policy issues remain unresolved, schools still need student data to conduct daily operations and provide core educational instruction. This section categorizes how schools use student data, distinguishes between primary and secondary uses and identifies uses that warrant specific parental and student consent. We divide schools' uses of student data into four categories: (1) **administrative uses**, (2) **instructional uses**, (3) **education assessment and measurement uses,** and (4) **other optional or non-education categories**.[10]

10 We recognize that this categorization may not provide a comprehensive taxonomy of data use in schools. For example, the Center of Law and Information Policy proposed breaking down the types of cloud services used by schools into seven categories, including school functions, classroom functions, student reporting and guidance. Joel Reidenberg et al., Privacy and Cloud Computing in Public Schools, Center on Law and Information Policy 17 (2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip. However, this categorization provides a starting point to conceptualize student data use and consent generally.

Administrative uses of student data are necessary for the everyday functioning of schools. Student information is used in order to facilitate student registration, class scheduling, guidance counseling, and keeping classroom attendance. Student data is needed to administer school lunch programs and busing services. Currently, schools share student data with various service providers, which provide software and data security and handle technical support. Such administrative functions facilitate and support schools' core educational mission.

Student data is also essential for classroom instruction. Increasingly, teachers use technology and online services to support classroom learning. Students use online services to complete homework assignments, work collaboratively, and engage with their teachers and classmates. Teachers want to use online-learning programs to let them direct what students work on *and* can automatically adjust to student needs.[11] New technologies not only enable personalized learning solutions that are tailored for every individual student, but they also can also improve how teachers engage with students one-on-one.[12] But tailoring course curricula and improving teacher-student interactions to maximize student learning generates massive amounts of data; this requires schools to rely on technology providers, data management and analysis experts, and other support services.[13]

Though there may be concerns about the efficacy of so much technology in the classroom, student data is clearly being collected and used for instructional purposes. Everyone understands that the context in which student data is collected is to facilitate a student's education;[14] indeed, using student data in this fashion is one of the key reasons schools need data in the first place.

Similarly, student data is also an essential tool to assess and measure the quality of education in schools.[15] Student assessment data can provide timely feedback to teachers and schools to understand and address each student's unique

---

11 Julia Freeland & Alex Hernandez, Clayton Christensen Institute, Schools and Software: What's Now and What's Next? i-ii (2014), http://www.christenseninstitute.org/wp-content/uploads/2014/06/Schools-and-Software.pdf.

12 Alan Schwarz, *Mooresville's Shining Example (It's Not Just About the Laptops)*, N.Y. Times (Feb. 12, 2012), http://www.nytimes.com/2012/02/13/education/mooresville-school-district-a-laptop-success-story.html.

13 Michelle R. Davis, *Schools Use Digital Tools to Customize Education*, EdWeek (Mar. 14, 2011), http://www.edweek.org/ew/articles/2011/03/17/25overview.h30.html

14 A context-based approach to privacy was first explored by Professor Helen Nissenbaum, and the principle endorses evaluating data use based upon what individuals might expect given the circumstances of collection. It has since been embraced by the White House's Consumer Privacy Bill of Rights.

15 While student data should be used to the benefit of the students, we must recognize that the analysis and use of student data may only indirectly benefit individual students. Use of student data for assessment and measurement may provide a bigger benefit to teachers and school systems and ultimately society at large than it will for any individual student. When it comes to data projects, better data benefit analysis is warranted.

learning needs, and can be important to identifying students who have special needs or academic gifts. Measurement data is also essential to improve and reshape teaching methods, course curricula, and classroom materials.[16] Nearly every educational improvement effort or initiative depends on analyzing individual student information in order to measure effectiveness.[17] In Kentucky, for example, regular high school feedback reports have altered how schools grade final exams and assign reading homework. "You can't improve preparation for college if you don't measure how kids are doing across the pipeline," explains the executive director of Kentucky's education data collaborative.[18]

Type of Use	Example
Administrative	Course scheduling, school busing
Instructional	Online homework, learning apps
Assessment and Measurement	Standardized tests, course assessments
Optional and Non-Educational	School yearbooks, PTA fundraising

While much of this student data is used as it has always been, many of these essential educational functions rely on the use of outside service providers or new technologies. Using vendors or new technologies is not new to the education space, but nonetheless, there are worries that the combination of more technology – and more student data as a result – and a reliance on school service providers has made it easier for student to data to be used inappropriately.

The final category of data uses to address are those marketing, advertising, or other non-educational uses of student data by third parties. Student directory information, for example, can sometimes be used for a variety of marketing, advertising, or other similar non-educational purposes, and is frequently given to companies that manufacture class rings or public yearbooks. This category of uses should require additional parental choice, and the ability to opt-out of these uses is appropriate.

THE CHOICE DEBATE

The introduction of new technologies and new uses of data in schools have generated new worries about how best to protect student privacy. These concerns are wide-ranging. Without considering how technology and data are

16 Analyzing Student Data, Pearson, http://www.pearsonschoolsystems.com/solutions/dataanalysis/ (last visited May 15, 2014).

17 E-mail from Daniel Domagala, Chief Information Officer, Colorado Department of Education, to Future of Privacy Forum (May 7, 2014) (on file with author).

18 Caralee J. Adams, *Data Driving College Preparation*, EdWeek (Nov. 15, 2011), http://www.edweek.org/ew/articles/2011/11/16/12data_ep.h31.html.

used in schools, some critics have focused their concerns on whether outside service providers or vendors may be improperly "mining" or selling student data.[19] Others worry about advertising or marketing in schools.[20] This comes on top of concerns about the security of student data or the risk of data breaches.[21]

Politicians have responded to these concerns with numerous legislative proposals across the country that attempt to address privacy concerns around student data. Many of these bills focus on governance measures, such as implementing chief privacy officers that can ensure privacy accountability at the state-level, but other proposals attempt to discourage the collection and use of data, specifically through new opt-in or opt-out requirements.[22] Offering additional opportunities for parental choice attempts to address a number of different but related concerns about (1) data generated by new technologies that, while used by students and teachers, is in the hands of outside service providers, and (2) more broadly, data collected by schools, districts, and state education agencies that are used for assessments and to track education outcomes over time.

Parents play an essential role in education, and when it comes to the technology implementation and planning process at schools and school districts, they should be consulted and invited to participate in the decision-making process. However, many of these choice proposals may not actually bring parents into the decision-making process *or* meaningfully improve student privacy. Individual parents are not in a position to become independent technology auditors or learning pedagogy specialists in order to make the best possible choice about day-to-day educational instruction.

According to Professor Joel Reidenberg, who has been sharply critical of how schools have handled student privacy issues, providing opt-out mechanisms will not solve the problem because the "complexity and sophistication of the data uses would make it difficult for the average parent to know what they're consenting to."[23] Elaborate consent requirements will overwhelm parents – and

---

19 Stephanie Simon, *Big Brother: Meet the Parents*, Politico (June 5, 2014), http://www.politico.com/story/2014/06/internet-data-mining-children-107461.html.

20 Press Release, While Policymakers Do Little, Marketers Are Busy in Schools, National Education Policy Center (Mar. 11, 2014), http://nepc.colorado.edu/newsletter/2014/03/schoolhouse-commercialism-2013

21 Benjamin Herold, *Danger Posed by Student-Data Breaches Prompts Action*, EdWeek (Jan. 22, 2014), http://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html.

22 Andew Ujifusa, *State Lawmakers Ramp Up Attention to Data Privacy*, EdWeek (Apr. 15, 2014), http://www.edweek.org/ew/articles/2014/04/16/28data.h33.html. Other bills blanket prohibitions on the collection of some categories of information.

23 Ellis Booker, *Education Data: Privacy Backlash Begins*, Info. Week (Apr. 26, 2013), http://www.informationweek.com/education-data-privacy-backlash-begins/d/d-id/1109713?.

could seriously impair how schools function. Professor Dan Solove, who has also taken issue with how student data is protected, is skeptical of the ability of consent alone to meaningfully protect privacy. Demanding parental consent will only lead to "more buttons to click and more forms to sign," which is compounded by the fact that most people hold "woefully incorrect assumptions about how their privacy is protected."[24]

Unintended Consequences of Mandating Consent

- Administrators have to manage multiple systems to provide basic services.
- Teachers find classrooms divided between some students who are permitted to use various educational tools and others who are not.
- Students miss out on accessing valuable educational content.
- The results of classroom, school, and district assessments become skewed.

IMPLICATIONS OF ADDITIONAL PARENTAL CHOICE

Though well-meaning, parental consent requirements can place significant burdens on schools, and some of the legislative proposals being offered could have serious, unintended consequences, impacting school administration, day-to-day instruction, and any assessment of the quality of our education system.

IMPACT ON SCHOOL ADMINISTRATION

Some proposals would require parental consent before any party can access or use student data, restricting even basic administrative tasks. As the Education Commissioner of New York explained, restrictions on basic information sharing would "render virtually impossible – or extraordinarily more expensive – much of the day-to-day data management of schools." [25] Schools would have to implement a bewildering assortment of different permissions.[26] Administrators

24 Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1886, 1899 (2013).

25 Andrew Ujifusa, *Student-Privacy Protection Focus of New York State Legislation*, EdWeek (June 17, 2013), http://blogs.edweek.org/edweek/state_edwatch/2013/06/student-privacy_protection_focus_of_new_york_state_legislation.html.

26 Andew Ujifusa, *State Lawmakers Ramp Up Attention to Data Privacy*, EdWeek (Apr. 15, 2014), http://www.edweek.org/ew/articles/2014/04/16/28data.h33.html. Other bills blanket prohibitions on the collection of some categories of information.

would need to treat students differently based not on their educational needs but on whether a student's data could ever pass out of their hands. The alternative would be to place administrators in the untenable position of needing to conduct basic administrative tasks with pen and paper, keeping records on index cards, or otherwise abandoning the use of technologies that make administration less time-consuming and more efficient.[27]

IMPACT ON INSTRUCTION

A system where each student has different permissions for each use of his or her data will have an enormous impact not just on school administration, but also on basic classroom instruction. Poorly considered consent requirements will take away learning opportunities from students. Students want a classroom environment that matches how they already use digital tools outside of school, [28] but consent requirements will invariably hamper access to those technologies in the classroom. Personalized learning, in particular, will be difficult to implement as it relies on data from many different sources to function.

The development of these tools holds a tremendous amount of potential to reshape and improve education. Companies are creating adaptive courses of study to keep students engaged and learning, and personalized learning is driven by student data, which includes not just traditional classwork but also student attendance and behavior information, educational assessments, and school- and district-wide assessments. [29]

Further, the need to manage classrooms where certain students have access to certain instructional materials or technologies could create a logistical crisis for teachers. In individual classrooms, one student might be able to access could access online services, remotely use online textbooks, or otherwise take advantage of in-classroom technology while another student could not. Taken to the extreme, individual students might be able to access one educational tool but not another, throwing a teacher's lesson plans into disarray. Teachers and administrators would have to constantly juggle classrooms and teaching instruction to account for which students are allowed to do what.

---

27 Benjamin Herold, *Q&A: Data, Privacy, and Parental Consent with Lori Fey of Ed-Fi Alliance*, EdWeek (Mar. 4, 2014), http://blogs.edweek.org/edweek/DigitalEducation/2014/03/qa_data_privacy_and_parental_c.html

28 Trends in Digital Learning: Students' Views on Innovative Classroom Models 9, Project Tomorrow & Blackboard Inc. (2014), http://www.tomorrow.org/speakup/2014_OnlineLearningReport.html.

29 *See* Sharnell Jackson, Using Data to Inform and Personalize Learning, available at www.edweek.org/media/071813_usingdata.pdf (last visited May 15, 2014); *but see* What Works Clearinghouse, Intervention Report: Carnegie Learning Curricula and Cognitive Tutor, Institute of Education Sciences (2013), http://ies.ed.gov/ncee/wwc/pdf/intervention_reports/wwc_cogtutor_012913.pdf.

IMPACT ON EDUCATION ASSESSMENT AND MEASUREMENT

Education systems rely on student data in order to assess students, teachers, and even classroom curricula.[30] Essentially most educational advances will depend on student information in order to measure effectiveness and to determine the best improvement strategies. Opt-outs may bias or otherwise limit the sample sizes needed to plot a course forward, effectively compromising the ability of state and local officials to accurately measure education outcomes.[31] When a significant portion of students are missing from a sample, any results would be skewed. This affects the ability to accurately evaluate educational programs, and potentially impacts the distribution of federal education grants and services, further hurting those schools and students most in need.[32]

EXACERBATING INEQUALITY

Policymakers focused on the goal of bridging educational inequalities are increasingly looking at technology as a way to close the gap.[33] Improving educational outcomes has long been a core public policy challenge, and despite decades of education reforms and increased spending, inequities continue to exist across much of our educational system from graduation rates and basic college readiness. Many of the new tools and efforts are aimed at discovering problems early on, measuring those problems, and then using technology to better understand how to best intervene on a student's behalf.[34]

Privacy advocates often worry that privacy will be based on socioeconomic class: the wealthy will pay for privacy-protection services, while the poor will be obligated to trade their data for free services.[35] In the education field, however,

---

30 Robert Kolker, *The Opt-Outers*, The New Yorker (Nov. 24, 2013), http://nymag.com/news/features/anti-testing-2013-12/index4.html (Quoting the New York State deputy education commissioner, cautioning parents "that if they remove their child from the assessment program, there's an impact. We really believe that these tests are not only important but irreplaceable. A parent who opts out of that is giving up the opportunity to get a critical piece of information.").

31 E-mail from Daniel Domagala, Chief Information Officer, Colorado Department of Education, to Future of Privacy Forum (May 7, 2014) (on file with author).

32 *See* Robert Kolker, *The Opt-Outers*, The New Yorker (Nov. 24, 2013), http://nymag.com/news/features/anti-testing-2013-12/index4.html. The consequences of opting-out of assessments in terms of either federal funding or producing misleading results is, at the moment, unknown, but could be significant.

33 Gene Sperling, National Economic Council, *Bridging the Digital Divide, From the Front Lines*, Wash. Post Live (Nov. 13, 2013), http://www.washingtonpost.com/postlive/bridging-the-digital-divide-from-the-front-lines/2013/11/12/95c14966-4b28-11e3-be6b-d3d28122e6d4_story.html.

34 *See* Terry M. Moe & John E. Chubb, Liberating Learning 2009.

35 Joseph Jerome, Buying and Selling Privacy Big Data's Different Burdens and Benefits, 66 Stan. L. Rev. Online 47 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/buying-and-selling-privacy

the converse may prove true, if efforts to demand opt-in or opt-out provisions for key education technologies are successful and leave the disadvantaged without access. Private schools are increasingly going "all in" with technology, taking advantage of new services to offer blended learning options and online classrooms for their students.[36] Affluent public school districts are also invested in bringing new technology into the classroom.

Lower income school children need every opportunity to access these same tools to identify their learning needs and to personalize opportunities for individual improvement if they are to compete with their peers. Access to technology is something that can function as a social equalizer if students from low-income neighborhoods can use the same digital content as students from upper-middle-class schools and districts.[37] But if parents are encouraged to opt-out or if less engaged parents simply do not opt-in to services, the very technology that is being proposed to narrow the educational divide could lead to that gap widening.[38]

SECURITY CONCERNS

Opt-out proposals are frequently designed to address worries about the use of cloud services in schools. The general worry is that cloud services create privacy and security risks simply by making data accessible via the web,[39] and as a result, parental consent should be necessary before school's take that risk. Alternatively, some critics have suggested that schools simply host their own systems instead of relying on outside digital storage or email services. Many school districts do just this, but it comes with significant security responsibilities and other costs that stress the capacity of most schools and districts.

---

36 Sophia Hollander, Privacy School Goes All In With Tech, Wall Street Journal (Nov. 18, 2012), http://online.wsj.com/news/articles/SB10001424127887323353204578127104047173928?mg=reno64wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424127887323353204578127104047173928.html; *see also* Keeping Pace with K-12 Online & Blended Learning (2013), available at http://kpk12.com/cms/wp-content/uploads/EEG_KP2013-lr.pdf.

37 Gene Sperling, National Economic Council, *Bridging the Digital Divide, From the Front Lines*, Wash. Post Live (Nov. 13, 2013), http://www.washingtonpost.com/postlive/bridging-the-digital-divide-from-the-front-lines/2013/11/12/95c14966-4b28-11e3-be6b-d3d28122e6d4_story.html.

38 The integration of technology in schools must also be done carefully to avoid perpetuating biases and discouraging achievement. Educators and service providers must ensure that they remain sensitive to the diverse backgrounds of students even as they develop and use technologies in the classroom.

39 *See, e.g.*, Daniel Solove, *Educational Institutions and Cloud Computing: A Roadmap of Responsibilities*, HuffingtonPost (Nov. 18, 2012), http://www.huffingtonpost.com/daniel-j-solove/educational-institutions-_b_2156612.html; Jon Bernstein, *Cloud Computing Raises Student Privacy Concerns*, Catalyst Chicago (May 12, 2012), http://www.catalyst-chicago.org/news/2012/05/14/20113/cloud-computing-raises-student-privacy-concerns; http://www.informationweek.com/inbloom-educational-data-warehouse-wilts-under-scrutiny/d/d-id/1111089; Denise Harrison, *Is Cloud Computing a Credible Solution for Education?*, Campus Technology (Nov. 12, 2009), http://campustechnology.com/Articles/2009/11/12/Is-Cloud-Computing-a-Credible-Solution-for-Education.aspx?Page=3.

As many Fortune 500 companies holding sensitive banking or health data have determined, relying on the security protections of outside companies that can deploy hundreds of staff and first class security tools can far exceed the capabilities of individual companies. Compared to large businesses, schools have far less funding and technical expertise.[40] Even large school districts are hard pressed to keep up with the continual security alerts, patches, and updates needed to maintain secure systems of their own, and as a result, schools have seen a direct benefit by relying on the expertise of outside parties and remotely hosting student data.

Building and hosting more complicated data management tools that offer detailed learning analytics becomes an even more challenging proposition for schools.[41] For schools to, in effect, opt out of using these services simply because parents are given the option to opt out does little to protect student privacy. Schools should not need to use their own employees to build their own data centers, develop their own educational apps and platforms, and run their own email systems – let alone do so securely – and it would be counterproductive for them to do so.

FERPA AND CHOICE

The Family Educational Rights and Privacy Act (FERPA) is the chief federal law that protects student privacy. Enacted in 1974, the law was designed to address "frequent, even systematic violations of the privacy of students and parents by the schools . . . and the unauthorized, inappropriate release of personal data to

40 These challenges are compounded by the wide-ranging differences in the size and wealth of individual school districts. The decentralization of education has proven problematic in the field of information technology. For example, in Oklahoma, education officials viewed consolidating information technology functions across the state as a key way to lower costs: Michael McNutt, *Oklahoma Officials Offer Consolidation of Information Technology Services to School Districts*, NewsOK (Feb. 7, 2013), http://newsok.com/oklahoma-officials-offer-consolidation-of-information-technology-services-to-school-districts/article/3753067.

41 Ben Kamisar, *InBloom Sputters Amid Concerns About Privacy of Student Data*, EdWeek (Jan. 7, 2014), http://www.edweek.org/ew/articles/2014/01/08/15inbloom_ep.h33.html ("The issue is, now we have to either build or do [a request for proposals] for 'middleware'—"data-management tools similar to what inBloom provides—"because you need storage of data, and you need learning analytics that integrate the data and connect it to standards and grade-level expectations," Ms. Stevenson said. "When you are going to do the work from scratch, it's a whole different world.") In these cases, the technical expertise is not so much about security, but about engineering, as well as software and instructional design; and the resource capacity is more about scale across multiple users both to support the development investment as well as the continuous improvement.

various individuals and organizations."[42] The law specifically gives parents the right to access and challenge incorrect school records about their children.[43]

The structure of FERPA contemplates where and when offering choice and requiring consent is appropriate. As a general rule, disclosing student data contained in educational records is prohibited without written consent. However, there are a number of important exceptions that to permit schools to disclose personally identifiable information (PII) from education records without consent.[44] These exceptions largely track how we categorized the types of activities that schools are engaged in.

School Officials under FERPA

FERPA allows schools to share data with entities they designate as "school officials."

Service providers may be designated school officials if they:

- **Perform institutional functions for which the school would otherwise use its own employees.**
- **Function under the direct control of the school or district with respect to the use and maintenance of education records.**
- **Use any student information only for purposes authorized by the school.**

SCHOOL OFFICIALS: ADMINISTRATIVE AND INSTRUCTIONAL USES

In order to facilitate basic educational activities, FERPA allows for data to be shared among school officials without parental consent. Because FERPA lacks an explicit "data sharing" provision,[45] schools rely on an exception that allows for disclosures of student information to entities designated as "school officials."[46] School officials are engaged in the core administrative and instructional activities of education, and they can include contractors, consultants, and even approved volunteers to whom a school has

42 Chrys Dougherty, *Getting FERPA Right: Encouraging Data Use While Protecting Student Privacy*, *in* A Byte at the Apple: Rethinking Education Data for the Post-NCLB Era 38, 39 (Marci Kanstoroom & Eric Osberg eds., 2008).

43 U.S. Dep't of Education, FERPA General Guidance for Parents, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html (last modified Apr. 10, 2014).

44 The Department of Education considers personally identifiable information (PII) to include, but not be limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record;(e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. 34 CFR § 99.3.

45 Privacy Technical Assistance Center, Transcript: Data Sharing Under FERPA (Jan. 2012), http://ptac.ed.gov/sites/default/files/data-sharing-webinar-transcript.pdf.

46 34 CFR § 99.31(a)(1)(B).

outsourced institutional services or functions.[47] As a result, tutors, cafeteria services, and increasingly, information technology providers receive data under the school official exception.

These outside parties, however, can only be considered as a "school official" if they meet certain requirement.[48] First, they must perform an institutional function for which the school would otherwise use its own employees. Second, the vendor needs to be under the direct control of the school or district with respect to the use and maintenance of education records. Finally, the outside party must use any student information only for authorized purposes and cannot re-disclose PII from educational records for any other purpose. These restrictions are generally established by a written agreement with the school, and the use of student data for a third party's own marketing activities cannot be considered a "legitimate" educational interest.[49]

By sharing data with a vendor or other school employee under the "school official" exceptions, the school does not grant unlimited access to education records.[50] The outside party must have a legitimate educational interest in the educational records. Schools or districts must establish criteria as to what constitutes a "legitimate educational interest," and provide this information to parents and students in an annual notification of FERPA rights.[51] The existence of a legitimate educational interest can be determined on a case-by-case basis.[52]

AUDIT OR EVALUATION EXCEPTION: STUDENT ASSESSMENT

In order to facilitate educational reporting requirements and to provide educators with the information needed to assess and evaluate education programs supported by state or federal funding, the audit or evaluation exception allows schools to share student data without consent.[53] The Department of Education has clarified that this exception allows schools to

---

47 *Id.*

48 34 CFR § 99.31(a)(1)(B)(1-3).

49 *See* Harrison Stark, *Protecting Student Data From the Classroom to the Cloud*, Common Sense Media (Feb. 26, 2014), https://www.commonsensemedia.org/educators/blog/protecting-student-data-from-the-classroom-to-the-cloud (noting that leading educational technology providers, including McGraw-Hill, Microsoft, and Amplify, all agreed that student data must only be used for "educational purposes.").

50 Defining "Legitimate Educational Interests," National Center for Education Statistics, http://nces.ed.gov/pubs2004/privacy/section_4b.asp (last visited May 15, 2014).

51 34 CFR § 99.7(a)(3)(iii).

52 Defining "Legitimate Educational Interests," National Center for Education Statistics, http://nces.ed.gov/pubs2004/privacy/section_4b.asp (last visited May 15, 2014).

53 34 CFR §§ 99.31(a)(3) and 99.35.

engage with outside service providers to help run and support state-wide longitudinal data systems.[54]

As discussed above, student assessment data is essential to evaluating not only student performance, but the quality of education generally. Longitudinal analysis promises to more accurately capture students' educational gains by following student performance over time – and this data allows schools to adapt to the educational needs of students transferring from school system to school system.[55]

In order to safeguard student privacy, FERPA regulations mandate that schools have written agreements with anyone receiving student data under this exception. While these agreements over schools a degree of flexibility, any written agreement *must* require that any personal information be destroyed upon completion of any evaluation or audit as well as require the implementation of policies and procedures to protect student data from any unauthorized uses.[56]

DIRECTORY INFORMATION: OPTIONAL AND NON-EDUCATIONAL

Another exception to FERPA allows schools the discretion to share "directory" information about students. While this information can be used for non-educational purposes, parents must be informed by the school what information is specifically considered "directory" information and offered the ability to opt-out of any sharing.[57] Parents are provided with notice that typically explains that "directory information" is often published in school play programs, the annual yearbook, a public honor roll, graduation programs, or basic sports activity flyers, showing the height and weight of team members.[58] Basic contact information could also be needed for companies that sell students class rings or yearbooks.[59] Offering parents these sorts of controls over directory information makes sense. Sharing this sort of information is optional and not essential to a school's educational mission.

---

54 76 Fed. Reg. 75604 (Dec. 2, 2011).

55 *See, e.g.*, Longitudinal Data System for Education in Maryland, Maryland State Department of Education (2009), http://www.marylandpublicschools.org/NR/rdonlyres/841ABD3D-FC95-47AB-BB74-BD3C85A1EFB8/20240/fact83.pdf

56 34 CFR §99.35(a)(3).

57 See 34 CFR § 99.37 for a discussion of the conditions needed for schools to disclose directory information.

58 U.S. Dep't of Education, Model Notice for Directory Information, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html (last modified Mar. 14, 2011).

59 E.g., Valley R-VI School District, Missouri, Notice of Designation of Directory Information (Nov. 2010), http://valleyschooldistrict.org/filestore/Form2400.pdf

Type of Use	Example	FERPA Disclosure Exception
Administrative	Course scheduling, school busing	"School Official"
Instructional	Online homework, learning apps	"School Official"
Assessment and Measurement	Standardized tests, course assessments	"Audit or Evaluation"
Optional and Non-Educational	School yearbooks, PTA fundraising	"Directory Information"

While privacy critics and some parent groups are worried that a lack of clarity in FERPA potentially allows for the sharing and use of student data for inappropriate marketing purposes, sharing of directory information has been singled out as particularly problematic.[60] Critics worry that parents either do not read or routinely ignore FERPA notices,[61] and as a result, parents are unaware of their options for the disclosure of directory information. However, schools are not obligated to make directory information available to any entity that requests it. In 2011, responding to the fact that some school districts had no directory information policies in place, the Department of Education released new guidelines that clarified that schools and districts could limit either who can access directory information or what they can do with this data.[62]

PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA)

Similarly, the Protection of Pupil Rights Amendment (PPRA) restricts non-educational uses of student data by offering parents additional choices.[63] It augments the protections of FERPA by giving parents an opportunity to review curriculum materials as well as requires explicit parental consent before students can participate in any kind of government-funded survey, analysis, or evaluation covering particularly sensitive topics ranging from political and religious affiliations to sexual attitudes and behaviors.[64]

---

60 Opt-Out Ferpa, http://www.opt-out-now.info (last visited May 15, 2014). *See also* Anya Kamenetz, *What Parents Need To Know About Big Data And Student Privacy*, NPR (Apr. 28, 2014 11:58 AM ET), http://www.npr.org/blogs/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy ("The big hole in FERPA is directory information," says Sheila Kaplan, the privacy activist.)

61 Winona Zimberlin, *Who's Reading Johnny's School Records?* (Apr./May 2006), *available at* http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/whosreadingrecords.html.

62 U.S. Dep't of Education, December 2011 - Revised FERPA Regulations: An Overview for SEAs and LEAs 2 (2011), *available at* http://www2.ed.gov/policy/gen/guid/fpco/pdf/sealea_overview.pdf ; 76 Fed. Reg. 19726-19739 (Apr. 8, 2011).

63 20 U.S.C. § 1232h (1978)

64 20 U.S.C. § 1232h(a-b).

It also addresses explicit marketing activities in schools. Schools are required both to warn parents in advance of any collection of data from students for marketing, and provide parents with an opportunity to review in advance and opt-out of any specific marketing efforts.[65] Yet PPRA recognizes that some marketing activities are also educational, and it shows how notice and opt-outs could hamper many activities that teachers as well as policymakers support. As a result, it excludes from PPRA's general marketing protections the following: (1) college, postsecondary education, or military recruitment; (2) book clubs, magazines, or other programs providing access to low-cost literacy products; (3) curriculum and instruction materials; (4) tests and assessments used to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students; (5) the sale by students of products for school or education-related fundraising; and (6) student recognition programs.[66]

THE ROLE OF VENDORS

Despite these long-standing exceptions, vendors who are entrusted with student data have become the subject of some of the most heated privacy debates about student privacy today, even as many of these vendors are providing essential school services.[67] Relying on vendors has become a standard business practice,[68] and organizations, including schools, use vendors when renting space, hiring contractors, or whenever they need to rely on outside expertise to handle a task. These relationships all require access to data.

Vendors have become even more essential as technology has entered classrooms and school houses. Under tight budgets, schools have turned to enterprise software to improve administrative efficiency and therefore reduce costs.[69] Scheduling, testing, remote learning, email services, and teacher dashboards are all services where schools seek services from vendors. They do so, in part, because both the sophisticated software and the complicated technical infrastructure needed to support these activities require considerable resources. School IT personnel are not equipped to develop and implement educational

---

65 20 U.S.C. § 1232h(b).

66 20 U.S.C. § 1232h(c)(1)(E).

67 Natasha Singer, *Group Presses for Safeguards on the Personal Data of Schoolchildren*, N.Y. Times, Oct. 13, 2013, http://www.nytimes.com/2013/10/14/technology/concerns-arise-over-privacy-of-schoolchildrens-data.html.

68 *Managing Data Security and Privacy Risk of Third-party Vendors*, Grant Thornton (2011), http://www.grantthornton.com/staticfiles/GTCom/Health%20care%20organizations/HC%20-%20managing%20data%20-%20FINAL.pdf.

69 Scott Aronowitz, Enterprise Software Brings Cost Savings to School Districts Worldwide, T.H.E. Journal (Sept. 24, 2009), http://thejournal.com/articles/2009/09/24/enterprise-software-brings-cost-savings-to-school-districts-worldwide.aspx.

software and services from scratch.[70] As a result, schools have followed the path of the private sector in relying on technology companies to provide these critical services. Education vendors range from for-profit start-ups to non-profit organizations. Some of these vendors are long time partners to the school system who have provided textbooks or testing on paper, but who now do so online, [71] such as Pearson, McGraw Hill Education, and Scholastic, while others are well known tech giants like Google and Microsoft who supply cloud based email services and storage systems. Many are new start-ups who are seeking to provide new ways for teachers to do their jobs better, and include small app developers, producers of adaptive instructional software, and educational content providers.

Data sharing with vendors is a common practice, and privacy laws in other sectors typically do not limit the sharing of data with vendors, particularly when a vendor acts under the control and at the behest of a first party, such as a hospital or bank. This is so because most organizations frequently need to have the ability to share data in order to accomplish basic tasks.

We see this across different privacy frameworks, including the European Data Directive, which recognizes privacy as a fundamental human right and places more controls on the collection and use of data that most countries. Even the Directive understands the important role vendors play. It nicely illustrates the division between first parties and vendors through the introduction of "data controllers" and "data processors."[72] While controllers determine the purposes and means by which data is used, processors engage in functions with personal data merely on behalf of a controller. In order to distinguish between the two, some aspects to look for include looking at the degree to which one party provides instructions or oversees the other, whether one party has a more visible relationship with an individual whose data is being used, and whether an individual should have expectations on the basis of this visibility.[73] As discussed above, the "school exception" in FERPA similarly works to place restrictions onto vendors.[74]

As a practical matter, relying on a courier to mail a letter is not generally considered sharing data with an outside third party, nor is providing data to one's lawyer or accountant. Loading data onto a computer server which happens to be

---

70 *See* Eric Butterman & Carol Patton, *Demystifying Cloud*, Scholastic Administr@tor Magazine, http://www.scholastic.com/browse/article.jsp?id=3755252 (last visited May 15, 2014).

71 *See* Jessica Leber, *The Education Giant Adapts*, MIT Technology Review (Nov. 23, 2012), http://www.technologyreview.com/news/506361/the-education-giant-adapts/.

72 Article 2 (d) and (e) of Directive 95/46/EC; *see also* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

73 *Id.* The EU Article 29 Working Party has also released an opinion about the privacy issues surrounding cloud computing available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

74 Further, we note that FERPA may only apply to a limited world of data. Any gaps in student data covered by FERPA should be addressed through legislative responses or better self-regulation.

hosted by a service provider describes a similar scenario. Without this concept of agency, a first party would need to have in-house expertise to fulfill every aspect of its activities. This is an expectation that no school district let alone school could meet, and it is a feat that is increasingly impossible for even the largest organizations.[75]

As a matter of pure terminology, labeling vendors as a "school officials" under FERPA is understandably confusing. FERPA went into effect just as traditional fair information practices were being established, and as a result, FERPA does not fully track with other traditional privacy concepts and later privacy legislation. Unlike newer privacy laws that govern health (Health Insurance Portability and Accountability Act) or financial (Gramm-Leach-Bliley Financial Modernization Act) data, the language in the FERPA statute lacks a clear notion of either a third-party vendor or a data processor that acts under the control of a school. While additional clarity may be warranted, other privacy laws demonstrate how consent requirements and choice are not an appropriate control for the use of vendors.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Access and sharing of health information presents important privacy questions, which Congress recognized when it passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. The law intended to create a uniform set of codes in order to more efficiently process insurance claims, and as a result of the greater ease in data sharing that would result, the law also directed the Department of Health & Human Services (HHS) to promulgate regulations with regard to the privacy of medical data. The final HIPAA Privacy Rule applies to protected health information (PHI) possessed by "covered entities," which include "health plans, health care clearinghouses, and health care providers."[76] However, as HHS acknowledges, most covered entities under HIPAA do not carry out all of their health care activities or other functions by themselves. They rely on the services of a variety of outside vendors.

The HIPAA Privacy Rule recognizes this. Regulations permit covered entities to disclose PHI to "business associates."[77] Examples of some of the functions provided by business associates include claims processing, quality assurance, billing, and data analysis or administration; services offered by business associates are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.[78]

---

75 Amy Malone, *Data: Big, Borderless and Beyond Control? Five Things You Can Do*, JDSUPRA (Mar. 3, 2014), https://www.jdsupra.com/legalnews/data-big-borderless-and-beyond-control-52884/.

76 45 C.F.R. § 160.102. Protected health information (PHI) under HIPAA consists of all "individually identifiable health information."

77 *See* 45 C.F.R. § 164.502.

78 45 C.F.R. § 160.103.

PHI can only be disclosed to these associates *if* the health providers or plans "obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule."[79] Furthermore, any disclosed information may not be used for the business associate's independent use or purposes.[80] Health providers can only disclose information to help themselves carry out their essential health care functions. As an added protection, business associates who violate HIPAA are subject to the same punishments as covered entities.

GRAMM-LEACH-BLILEY FINANCIAL MODERNIZATION ACT (GLBA)

Similarly, protecting the privacy of consumer financial information held by "financial institutions" is at the heart of privacy provisions in the Gramm-Leach-Bliley Financial Modernization Act (GLBA) of 1999. The financial privacy rules implemented by the GLBA provide consumers with privacy notices that explain the information-sharing practices of banks and other financial institutions, and give consumers rights to limit *some* sharing of their information.[81]

In general, GLBA requires consumers be given the right to prevent financial institutions from disclosing personal financial information to third-parties.[82] However, there are a number of important exceptions to this right that all include vendors. Specifically, individuals may not decline, or "opt-out" of information sharing in three scenarios. First, financial institutions can share data with nonaffiliated third parties in order to perform services for the financial institution or to function on its behalf, including marketing the bank's own products or services. Financial institutions are required to provide consumers with notice of the arrangement, and by contract, prohibit the third party from disclosing or otherwise using the information. Second, financial institutions are allowed to share data as necessary to administer consumer transactions such as audits of credit information, administration of rewards programs, or to provide an account statement. Finally, GLBA allows financial institutions to make disclosures to

---

79 U.S. Dep't of Health & Human Serv., Health Information Privacy, Business Associates, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last revised Apr. 3, 2003).

80 *Id.* It is worth noting, however, that business associates may be able to engage in data aggregation and business associate management independent of any agreement with a HIPAA covered entity. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,644 (Dec. 28, 2000).

81 Fed. Trade Comm'n, Bureau of Consumer Protection, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://www.business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act (last updated July 2002).

82 Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information) VIII-1.2, FDIC Complaince Manual (Jan. 2014), *available at* http://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf.

protect against fraud, to share with the institution's attorneys, accountants, and auditors, and to comply with any legal or regulatory requirement.

Whether through "business associates" or opt-out exceptions, our primary health and financial privacy laws recognize the need for third-party vendors to have controlled access to data. Offering individuals the choice to avoid having their information shared with vendors would make it impossible for any organizations to perform basic functions. Without being able to share data, health care providers would be unable to be accredited – or to use outside experts to de-identify health data.[83]

Rather than vendors, the third parties that privacy laws should concern itself with are entities that claim independent rights to use personal information. In the United Kingdom, for example, the Information Commissioner's Office specifically defines third parties in such a way to ensure that any vendor only authorized to process data on a first party's behalf "is not considered a third party."[84]

OPTING INTO SUCCESS

Under U.S. law, notice and choice have traditionally been viewed as the most fundamental principles to protect privacy.[85] Our privacy laws generally give individuals the right to stop certain sharing of their personal information. **However, rules around notice and choice must balance individuals' right to privacy with organizations' need to collect, use and share personal information for normal business purposes.[86]**

Schools are in the business of educating, and while schools should provide students and parents with better notice about how data is being used, mandating that they obtain consent to use data for educational purposes is counterproductive. Certainly, when student data can be used for non-educational purposes, choice is appropriate. In many cases, choice is already offered: both FERPA and PPRA provide parents and students with opt-out rights – FERPA from school release of directory information and PPRA from use of information for marketing purposes. The common thread tying together these opportunities to exercise choice is their involvement in data uses for *non-educational purposes*.

---

83 *Who is a HIPAA business associate?*, McDonald Hopkins Alert (July 3, 2013), http://www.mcdonaldhopkins.com/alerts/healthcare-who-is-a-hipaa-business-associate.

84 U.K. Information Commissioner's Office, Key Definition of the Data Privacy Act, http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions (last visited May 15, 2014) "In relation to data protection, the main reason for this particular definition is to ensure that a person such as a data processor, who is effectively acting as the data controller, is not considered a third party."

85 *See, e.g.*, Fed. Trade Comm'n, Privacy Online: A Report to Congress 7 (1998).

86 *See generally* Fed. Deposit Insurance Corp., Privacy Choices, http://www.fdic.gov/consumers/privacy/privacychoices/#yourright (last updated Jan. 25, 2008).

Different considerations come into play when data is shared strictly for educational purposes. Here, the goal of school officials – and vendors – should be to engender trust. Rigid notice and consent requirements fall short of creating trust between parents and schools around the use of student data.

More steps should be taken by schools, vendors, and other organizations in the education ecosystem to improve student privacy and address parents' concerns. Parents can and should be involved. Indeed, the original goals of FERPA were to provide parents with access to student records and the ability to correct inaccurate information. As data becomes increasingly prevalent in the assessment of student performance, ensuring access to such data becomes key. To be sure, non-educational uses of student data should require prior parental consent. But within the educational sphere, parents and students would be better served by better information about how student data is used, including more robust tools to access and harness than information. School officials are already working to make educational reports more accessible and visually friendly for parents.[87]

Type of Use	Is Choice Required?	Should Additional Notice and Transparency Be Provided?
Administrative	No	No
Instructional	No	Yes
Assessment and Measurement	No	Yes
Optional and Non-Educational	Yes	Yes

An adversarial relationship among schools, parents, and vendors is toxic in an educational environment. If vendors are regarded as being motivated to misuse student information rather than serving their users with the highest quality educational services, there is little hope for education technology. When it comes to technological advances, parents, students, and teachers must be on the same page.

Achieving this will require not only transparency, but also additional accountability mechanisms. Schools and third-party vendors must do more to enhance accountability for data sharing and use. Inappropriate commercial advertising and marketing uses must be limited, and vendors must be required to comply with FERPA's limits on "legitimate educational interests."[88] When concrete privacy concerns are identified, schools should protect all students' privacy, not just those students who might have opted-out of certain non-educational uses. For example, personalized learning tools

87 E-mail from Daniel Domagala, Chief Information Officer, Colorado Department of Education, to Future of Privacy Forum (May 7, 2014) (on file with author).

88 Ellis Booker, *Education Data: Privacy Backlash Begins*, Info. Week (Apr. 26, 2013), http://www.informationweek.com/education-data-privacy-backlash-begins/d/d-id/1109713?.

raise concerns about the leakage of student data profiles into the non-education and employment environments, limiting students' options as they transition into the working world.[89] Instead of allowing some students to opt-out of an otherwise promising development in education technology, such concerns are better addressed by restricting how data collected through personalized education technologies can be used. This way *every* student would receive the benefits *and* have his or her privacy protected.

Companies can do more on both the legal and outreach fronts.[90] Industry best practices remain in their infancy in education technologies; while there are efforts to establish industry guidelines, more work needs to be done.[91] Companies must ensure that their practices are more transparent, so that schools officials can make better judgments to assess whether they comply with FERPA requirements and contractual obligations.

In the meantime, state policymakers should consider privacy in a rational manner. They should disentangle student privacy issues from wider policy debates about education reform. They should begin by inventorying the data that is collected about students and designating accountable individuals to oversee its use.[92] State officials should ensure appropriate security practices and auditing of data use and designate a dedicated officer to oversee the process. New York, for example, has created a state-level chief privacy officer responsible for coordinating the protection of student data,[93] and other states are also exploring the idea.[94]

---

89 Gary Stern, *N.Y. Plans to Share Data From Pre-K to Workforce, Aims to Unlock Keys to Student Success*, LoHud.com (Jan. 25, 2014), http://www.lohud.com/article/20140125/NEWS02/301250047.

90 In a separate paper, Jules Polonetsky and Omer Tene elaborate on the need for parents and students to be granted access to student data in a useable format. Alongside further insight into the logic underlying the algorithms used to assess student performance, this sort of "featurizing" of data could help students and parents see how they are doing in real time – and help nurture students' strengths and support them in their weaknesses. Jules Polonetsky & Omer Tene, *Who Is Reading Whom Now: Privacy in Education from Books to MOOCs* 68-71 (2014) (working draft on file with author).

91 Mark Schneiderman, *SIIA Announces Industry Best Practices to Safeguard Student Information Privacy and Data Security and Advance the Effective Use of Technology in Education* (Feb. 24, 2014), http://www.siia.net/blog/index.php/2014/02/siia-announces-industry-best-practices-to-safeguard-student-information-privacy-and-data-security-and-advance-the-effective-use-of-technology-in-education/.

92 See iKeepSafe, Student Data Privacy and Security: A Roadmap for School Systems, for a discussion of how school districts might implement privacy programs.

93 Press Release, Governor Cuomo and Legislative Leaders Announce Passage of 2014-15 Budget, Governor of N.Y. (Mar. 31, 2014), http://www.governor.ny.gov/press/03312014Budget

94 Andrew Ujifusa, *State Lawmakers Ramp Up Attention to Student Data Privacy*, EdWeek (Apr. 16, 2014), http://www.edweek.org/ew/articles/2014/04/16/28data.h33.html.

Secretary of Education Arne Duncan has suggested that student privacy rules "may well be the seatbelts of this generation."[95] At the same time, he recognized that schools must have the ability to utilize data to deepen and accelerate student learning. Offering parents legalistic notice and choice or allowing students to opt-out from educational uses of their data will not resolve this tension. Rather, parents must be included in all stages of the policymaking process and have a voice in the shaping of the goals of the education system and the tools that will be used to harness data in schools. Once those issues are agreed, all stakeholders will embrace uses of data that can help deliver educational success.

95 Arne Duncan, U.S. Sec. of Ed, Technology in Education: Privacy and Progress, Remarks at the Common Sense Media Privacy Zone Conference (Feb. 24, 2014), https://www.ed.gov/news/speeches/technology-education-privacy-and-progress.