Statement of Jules Polonetsky
Executive Director, Future of Privacy Forum

Written Testimony
Before the California State Assembly Joint Committee Hearing on
Ensuring Student Privacy in the Digital Age

May 14, 2014

The Future of Privacy Forum (FPF) is a think tank seeking to advance responsible data practices and is supported by leaders in business, academia, and consumer advocacy.[1] FPF believes that the collection, analysis, and use of personal data provide many benefits to both consumers and society, and that innovative uses for data will only increase in the future. However, we also recognize the risks of misuse of data and work to ensure the inappropriate uses of data are curtailed. As part of our portfolio of work, FPF has taken an interest in the benefits and risks of education data and technology.

We thank you for the opportunity to provide written comments, and hope our contribution informs the discussion of student privacy before the Joint Committees on Education and Privacy.

OVERVIEW

Education is changing – online curricula and tools proliferate; use of social media and cloud applications for file storage, note-taking and collaboration has become mainstream; student performance data is driving next-generation models of learning and measurements for teacher effectiveness; and connected learning is fast becoming a path for access and academic achievement. Information and data are flowing within schools and beyond, enabling new learning environments and providing much needed analytics to understand and improve the way teachers teach and students learn. Data is increasingly being used to hold schools and educators accountable for student performance.

[1]The views herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.

On the one hand, these new education technologies (ed tech) bring tremendous promise to the education world. They allow schools to customize programs and tailor them to individual students; make education more collaborative and engaging through social media, gamification and learning management systems; and facilitate access to education for anyone with an Internet connection in remote or underprivileged areas of the country. They allow students to broaden their horizons through openly available lectures from the best professors at world leading universities such as Stanford, Harvard and MIT, while also benefitting from automated individualized tutoring and adaptive learning tools that help strong students surge forward while not letting the weaker lag far behind.

At the same time, the confluence of enhanced data collection with highly sensitive, information about children and teens makes for a combustive mix from a privacy perspective. Some critics consider many ed tech efforts misguided, labeling them as the work of "corporate education reformers" seeking profits at the expense of public education. Technology and data have become a lightning rod for education counter-reformers who blame technology evangelists for worshipping data rather than valuing the professionalism of teachers and recognizing the social inequality that is often the real source of poor student performance. While perhaps not mutually exclusive, these advocates call instead for entirely different education solutions, focused on smaller classes and higher salaries for more qualified teachers. They argue that because of ed tech, students become addicted to screens, teachers are demoted to assembly line workers, classes are devoted to test preparation in place of education, and school systems obsess over numbers instead of student welfare.

The tension between ed tech opportunities and privacy and civil liberties concerns has been recognized by policymakers at the highest levels of government. In its recent report, *Big Data: Seizing Opportunities, Preserving Values* (the "White House Report"), the White House recommends that Congress "modernize the privacy regulatory framework under the Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) to ensure two complementary goals: 1) protecting students against their data being shared or used inappropriately, especially when that data is gathered in an educational context, and 2) ensuring that innovation in educational technology, including new approaches and business models, have ample opportunity to flourish."[2]

The debate is fraught with emotions, with teachers fearing for their jobs, parents anxious about their children's future, and schools worried, on the one hand, of being left out of funding opportunities and technological progress, and on the other hand, of exhausting already scarce resources on navigating an increasingly complex data ecosystems while avoiding data breaches or privacy snafus. The recent implosion amid a flurry of privacy allegations of inBloom, an ed tech high flyer funded by a $100 million grant from leading foundational supporters, is a testament to the toxicity of the current environment and the risks it bears for both vendors and schools.

[2] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, May 2014, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

PRIVACY CHALLENGES

Some of the privacy challenges that arise with the emergence of ed tech are common to other market segments and industries. They include concerns about outsourcing, vendor contracts, data security, and compliance with fundamental privacy principles. They require intricate distinctions to be made between commercial uses of data for marketing or for product improvement within and outside of the field of education. In addition to those challenges, ed tech features perplexing dilemmas arising from big data capabilities, including concerns over unfairness and discrimination, narrowcasting and filter bubbles, predictive sorting and the stratification of society. Yet other ed tech issues transcend the privacy debate and include highly politicized controversies around the role of the federal government in education, standardization through the Common Core, and the allocation of responsibilities between school administrators, teachers and parents.

Collection and use of students' data has always been key for effective administration of school systems. One commentator characterized schools as "information-collection machines," aggregating data about students' attendance, assignment and test results, grades and report cards, disciplinary records, guidance counselor assessments, disabilities and medical conditions, vaccinations, qualification for free lunches and more.[3] Schools have long collected and maintained essential, sensitive information about children – data needed to administer their core academic activities. In reality, education has long been data rich and information poor, collecting much information but in formats and silos that made it inaccessible and inactionable. But big data capabilities and a new influx of ed tech innovations have pushed the envelope by allowing educators to harness that information to inform decisions, in part upsetting the delicate balance between various stakeholder groups.

OUTDATED REGULATORY TERRAIN

Before the passage of FERPA in 1974, it was not clear which parties could access and share student data and what rights if any did parents have in their children's information. School newspapers and general media published information about which students made various sports teams, including such students' height and weight. Lists of graduates, as well as the names of students making the honor roll or winning awards, were often proudly featured in hometown newspapers. The names of winners of the Westinghouse Science Talent Search were broadcast on the radio. School yearbooks published information about students, including name, photos and various personal details. Parents volunteering at a school could learn information about students other than their child. A broad range of student data was collected and shared and often made public.

The rules on who could access student information were unclear and sometimes unfair. Police and health departments were granted easy access to student data, while parents were often denied access to their children's records, making it impossible for them to correct or challenge mistaken or stigmatizing information.

[3] Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public Schoolchildren*, 84 Neb. L. Rev. 1158, 1159 (2006).

Senator James Buckley led efforts to provide parents with access to student data in the shadow of the Watergate scandal, amid growing concerns about secret government files. Buckley said "[T]he concern that I had and that the committee chairman had was the practice of many schools to keep parents from having access to comments in school records affecting their own children. … That was the central concern, that parents would know what was being done about their children."[4] This concern frames and underlies the mechanism introduced by FERPA, but also forewarns its shortcomings.

FERPA Fundamentals

In 1974, merely twelve days after President Richard Nixon's resignation, the Buckley Amendment, known today as the FERPA, was signed into law by Nixon's successor, President Gerald Ford.[5] At its core, FERPA is a budget statute, which applies to educational agencies and institutions that receive federal funds administered by the Secretary of Education.[6] Accordingly, the sole sanction under the FERPA is the withdrawal of federal by the Department of Education. FERPA had two main goals: First, it was designed to ensure that parents were able to receive, review and, where necessary, correct all educationally related documents that could affect their child's educational progress. Second, it was intended to curtail the "frequent, even systematic violations of the privacy of students and parents by the schools . . . and the unauthorized, inappropriate release of personal data to various individuals and organizations."[7]

More specifically, FERPA's right of access gives parents the right to inspect and review their children's education records, as well as to challenge the content of the education records, to delete or change any inaccurate, misleading, and other information that otherwise violates the "privacy rights" of the student.[8] FERPA's restrictions on disclosure of student information provide that an educational institution can be financially penalized for a "policy or practice" of releasing "personally identifiable information" contained in educational records without written parental consent.

FERPA's nondisclosure provision is subject to a carve-out, allowing disclosure of "directory information" without prior parental consent, provided that parents are permitted to opt-out.[9] The

---

[4] Student Press L. Ctr., White Paper: FERPA and Access to Public Records (2010), http://www.splc.org/pdf/ferpa_wp.pdf.

[5] *See* U.S. Dep't of Educ., Legislative History of Major FERPA Provisions 1 (June 2002), http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpaleghistory.pdf.

[6] 34 C.F.R. § 99.1. Under FERPA, an educational agency or institution is "any public or private agency or institution which is the recipient of funds." 20 U.S.C. § 1232g(a)(3).

[7] *See* 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 39 (Marci Kanstoroom & Eric Osberg, eds., 2008).

[8] *See* 20 U.S.C. § 1232g(a)(4)(B); 34 C.F.R. §§ 99.10- 99.20.

[9] Directory information includes "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent education agency or institution attended by the student." 20 U.S.C. § 1232g(a)(5)(A). *See also* 34 C.F.R. § 99.3.

directory information exception is typically used by schools to publish yearbooks, phone directories, concert programs, sports teams' rosters, and the like. In addition, FERPA authorizes nonconsensual disclosure not subject to a parental opt-out to certain transferees related to the educational function of the institution, such as disclosures to a "school official" for "legitimate educational interests;" to other education agencies; to federal and state authorities for auditing and evaluating; and more.[10] Finally, FERPA prohibits re-disclosure of student information pursuant to an authorized disclosure.[11] Yet any transfer effected under a FERPA exception for nonconsensual disclosure is not considered a "disclosure" and therefore not subject to re-disclosure restrictions.[12] In other words, if a school shares student data with a vendor under the "school official" exemption, such vendor may share the data with another vendor as long as the data are used for the same purpose set forth by the school.[13]

FERPA's protections apply to students' "education records," defined as "records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution."[14] This definition suggests that only those documents affirmatively kept or collected by a school are protected by FERPA.[15] Moreover, the term was interpreted narrowly by the Supreme Court, which held in *Owasso Independent School District v. Falvo* that "peer grading," the practice of asking students to score each other's tests, papers, and assignments as the teachers explain the correct answers to the entire class, does not create "education records" because the grades are not "maintained" by a school.[16] The court held:

> "The word 'maintain' suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database, perhaps even after the student is no longer enrolled. The student graders only handle assignments for a few moments as the teacher calls out the answers. It is fanciful to say they maintain the papers in the same way the registrar maintains a student's folder in a permanent file."[17]

The court's narrow, formalistic approach is quite inapposite to the general conception of personally identifiable information (PII) in privacy regulation as any information about an identified or

---

[10] *See* 20 U.S.C. § 1232g(b)(1)(A)-(F).
[11] *See id.* § 1232g(b)(4)(B); 34 C.F.R. § 99.33.
[12] *See* 34 C.F.R. §§ 99.31; 99.33(b).
[13] Kathleen Styles, the chief privacy officer of the U.S. Department of Education, notes "The school or district could ask a cloud provider to re-disclose FERPA-protected information to another school official, such as an app developer, if that app developer also meets the criteria required for school officials (legitimate educational interest, etc.)." Daniel Solove, *Interview with Kathleen Styles, Chief Privacy Officer, U.S. Department of Education*, LINKEDIN (Apr. 17, 2013), https://www.linkedin.com/today/post/article/20130417111651-2259773-interview-with-kathleen-styles-chief-privacy-officer-u-s-department-of-education.
[14] 20 U.S.C. § 1232g(a)(4)(A). *Also see* 34 C.F.R. § 99.3 (definition of "education record"). Contrast this to the definition of the term "record" in the Privacy Act, 1974, enacted just a few months after the FERPA: "[A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).
[15] *See id.*
[16] Owasso Indep. Sch. Dist. No. I-011 v. Falvo *ex rel.* Pletan, 534 U.S. 426 (2002).
[17] *Id.*, at 433.

identifiable individual. To be sure, FERPA *also* introduces the term PII, prohibiting educational entities from releasing or providing access to "any personally identifiable information in education records."[18] FERPA defines PII to include direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name).[19] However, as Daniel Solove and Paul Schwartz point out, despite mentioning PII, FERPA central concept remains that of "education records."[20] Hence, as one commentator wrote, the *Owasso* ruling reflects a belief that FERPA was intended to combat "secret files," not to provide more generalized protection for students' personal information.[21]

Since the enactment of FERPA, education policy and technology innovation and adoption has changed dramatically. The emergence of data on student performance across the globe has led to a widespread understanding that American students were underperforming relative to their peers overseas. Data also confirmed the achievement gap, even in high-performing school districts, between poor and minority students and white and more affluent students. This drove federal and state education officials to place increasingly strong emphasis on collecting and using data to improve schools' and students' performance. The concept of an "education record" became outmoded. Indeed, the hallmark of big data is the escape of information from the confines of a structured database and the ability to harvest, analyze, rearrange and reuse freestanding information. Experts argue that even the term PII has reached its zenith given the ability to harness apparently unidentifiable information to track individuals. Moreover, the outsourcing of data warehousing and other data-enabled functions such as adaptive instructional software to technology vendors has become part and parcel with managing school information systems as opposed to an isolated event. As is the case with cloud computing more generally, customers in the education sector find themselves dealing with layers upon layers of service providers delivering infrastructure, platform and software solutions.

FERPA Shortcomings

As a result of these changes, Dan Solove called FERPA "old and ineffective,"[22] arguing the federal statute was "in dire need of reform, as demonstrated by its failure to address so many key issues

[18] 20 U.S.C. § 1232g(b)(2). While FERPA does not define PII, a federal regulation issued thereunder does. *See* 34 C.F.R. § 99.3 (defining PII as a student's name; address; personal identifier, such as a social security number, student number, or biometric record; "[o]ther indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;" and "[o]ther 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.").

[19] 34 C.F.R. § 99.3 (defining "personally identifiable information").

[20] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.Q. REV. 1814, 1822 (2011), *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs.

[21] Mary Margaret Penrose, *In the Name of Watergate: Returning FERPA to its Original Design*, 14 N.Y.U. J. LEGIS. & PUB. POL'Y 75, 91 (2012), *available at* http://www.nyujlpp.org/wp-content/uploads/2012/10/Mary-Margaret-Penrose-In-the-Name-of-Watergate-Returning-FERPA-to-Its-Original-Design.pdf. Notwithstanding Owasso, schools and vendors generally consider student personal information of any sort subject to privacy protections.

[22] Daniel Solove, *The Battle for Leadership in Education Privacy Law: Will California Seize the Throne?*, LINKEDIN (Mar. 31, 2014), https://www.linkedin.com/today/post/article/20140331063530-2259773-the-battle-for-leadership-in-education-privacy-law-will-california-seize-the-throne.

regarding the use of cloud computing services by schools and educational entities."[23] He noted that "HIPAA is far from perfect, but it leaves FERPA in the dust when it comes to the strength of its privacy and security provisions."[24] Critics point out many shortcomings of the FERPA regime. For starters, FERPA lacks of an effective enforcement mechanism absent an avenue for individual redress[25] and given the lack of Department of Education jurisdiction over non-school actors. Solove writes that the only remedy under FERPA is "a sanction so implausible it has never been imposed in the 35+ year history of the law. That sanction is a withdrawal of all federal funds. It will never happen."[26] Not only that, but FERPA also provides the Department of Education with the power to enforce only against schools as opposed to any downstream vendors. In the absence of a private cause of action, this means that once student data leaves the hands of a school, it is no longer covered by effective FERPA protection.[27]

We do note that the Department of Education does have some greater enforcement tools than critics have allowed. In some cases, the Department can ban an individual vendor from doing business with schools for 5 years. It can issue cease and desist orders and it can negotiate compliance agreements. And in *United States v. Miami University*,[28] the court found that FERPA expressly permits the Secretary of Education to bring suit to enforce the FERPA conditions in lieu of its administrative remedies. But given the historic lack of enforcement in this area, the concerns about enforcement shortcomings of FERPA are compelling.

Second, FERPA lacks a "vendor" concept causing schools to force contractors into the terminologically awkward category of "school officials." This means that a broad swath of vendors, ranging from cafeteria operators to bus companies to cloud storage providers, get lumped together with teachers, principals and administrators under the category of school officials. Third, FERPA provides little to no guidance about data governance and security obligations. Apparently, vendors are not required to put in place a data breach response plan, much less a comprehensive privacy and data security program that is audited and enforced by an education institution. These shortcomings add to the definitional issues discussed above, such as FERPA's application strictly to "education records."

Moreover, developments on the ground require modification of some of the FERPA provisions to better reflect current technological and business realities. Consider, for example, one of the fundamental rights afforded by FERPA – the rights of parents to review and amend their children's education records. These rights reside with parent until a student turns 18 years old or enters a post-secondary institution, at which point they transfer from the parents to the student. In the past,

---

[23] Daniel Solove, *FERPA and the Cloud: What FERPA Can Learn from HIPAA*, SAFEGOV (Dec. 17, 2012), http://www.safegov.org/2012/12/17/ferpa-and-the-cloud-what-ferpa-can-learn-from-hipaa.
[24] *Id.*
[25] *See* Gonzaga University v. Doe, 122 S. Ct. 2268 (2002) (holding FERPA creates no personal rights enforceable through federal lawsuits).
[26] Solove, *FERPA and the Cloud*, *supra* note 23.
[27] *See* Daniel Solove, *Big Data and Our Children's Future: On Reforming FERPA*, LINKEDIN, https://www.linkedin.com/today/post/article/20140507051528-2259773-big-data-and-our-children-s-future-on-reforming-ferpa.
[28] United States v. Miami University, No. 00-3518, 2002 U.S. App. LEXIS 12830, (6th Cir. June 27, 2002).

such records typically contained a student's transcript as well as assessments by teachers. Yet the revolution in data collection and storage capabilities has facilitated access to information that is at once more comprehensive and more granular. For example, school records may contain information such as a student's participation in a LGBT club, or information shared in confidence with a guidance counselor. Teen students in particular may expect some degree of confidentiality to protect against parent access to such information.[29] FERPA fails to account for such nuance. And while parents should certainly be able to review their child's grades and other important records, it is not clear that they should be able to debate or contest every item of data recorded.[30]

Or take FERPA's limitations on disclosure of student data to third parties. Some of the information locked down in school databases is of great interest and value to the cause of civil rights organizations and education reformers, who strain to access accurate data about the prospects and performance of students from underprivileged populations. Civil rights investigators have recently revealed, for example, school disciplinary policies that disproportionately affect minorities. In its editorial, the *New York Times* wrote "documents included striking data on racial inequities. For example, African-American students represent only 15 percent of public school students, but they make of 35 percent of students suspended once, 44 percent of those suspended more than once and 36 percent of those expelled."[31] There is a compelling public interest to ensure the continued flow of such information.

Critics argue that rather than to protect children's privacy, schools use FERPA as a shield against disclosing unfavorable information. Mary Margaret Penrose wrote, "For years, schools have been hiding behind FERPA and intentionally preventing disclosure of records to third parties …. "[32] Indeed, Senator Buckley, the drafter of the law himself, derided such use of FERPA, stating "That's not what we intended. The law needs to be revamped. Institutions are putting their own meaning into the law."[33] Similar tensions accompany attempts to access student information at higher education institutions. The New America Foundation is leading a push to liberate data from colleges and universities in order to rate schools based on objective parameters such as access, affordability, and outcomes. This, in turn, will help rationalize the allocation of federal grants of funding and of student enrollment.[34]

---

[29] *See* Stuart, *supra* note 3, at 1162-69 (discussing and critiquing the extensive rights FERPA affords parents).

[30] The concerns raised here are not intended to cast doubt on the desirability of FERPA's access and amendment provisions, but rather to point out that critics who argue that every file a school has should be accessible potentially ignore some of the subtlety.

[31] Editorial Board, *The Civil Rights of Children*, N.Y. TIMES (Jan. 11, 2014), http://www.nytimes.com/2014/01/12/opinion/sunday/the-civil-rights-of-children.html.

[32] Penrose, *supra* note 21, at 96.

[33] Jill Riepenhoff & Todd Jones, *Secrecy 101: College Athletic Departments Use Vague Law to Keep Public Records from Being Seen*, COLUMBUS DISPATCH, May 31, 2009, http://www.dispatch.com/content/stories/local/2010/10/14/secrecy-redirect.html.

[34] *See* Clare McCann& Amy Laitinen, New America, Education Policy Program, College Blackout: How the Higher Education Lobby Fought to Keep Students in the Dark (March 2014), http://www.insidehighered.com/sites/default/server_files/files/CollegeBlackout_March10_Noon.pdf.

State Laws

In the absence of Congressional action and in the face of accelerating technological change and rising public outcry, state legislatures have weighed in with a flurry of legislative proposals from New York[35] to Louisiana,[36] to Oklahoma[37] to California.[38] These laws attempt to close loopholes and perceived weaknesses in existing privacy regulation. Alas, given the political pressure to act expeditiously, they often reflect an overreaction on the part of lawmakers and present crude solutions at the price of new problems. A patchwork of state laws also poses a challenge to stakeholders working across states to the degree there are differences in definitions (e.g., student data) and requirements (e.g., security standards and third party uses).

An approach advanced by Digital Learning Now and the American Legislative Exchange Council (ALEC), and adopted in Oklahoma and partially in New York, requires states to put in place data governance systems, including the appointment of a chief privacy officer, setting forth data management policies, and introducing periodic assessments and audits to verify compliance.[39] Such initiatives reflect necessary sensible first steps to help take stock of the range of data collection and use practice as well as existing privacy and security norms, before states react to concerns raised in the heat of a generalized public backlash to testing standards, Common Core and other debates around education reform.

Currently, many schools and school districts do not have the legal, technical and policy expertise to identify and manage emerging privacy risks, let alone respond to a range of new legal requirements. Efforts led by the Consortium for School Networking (CoSN), National School Board Association, Harvard Berkman Center for Internet and Society, Common Sense Media and Internet Keep Safe Coalition (iKeepSafe), seek to provide guidance to help schools navigate the current privacy regime and create tools to enable compliance. These steps need to be expanded, so that policymakers can soberly assess the most effective legislative path to fill education privacy gaps, while not impeding a vibrant environment of digital learning.

COMMERCIALIZATION

Engaging Tech Vendors

To date, the most heated privacy debates about student data have not focused on sharing information with the public or unaffiliated third parties or with parental access to school records. Rather, the discussion has centered on access to and use of data by vendors who provide schools with various services, ranging from school bus and cafeteria facilities to sophisticated data analysis tools. The rhetoric has been virulent, with critics accusing vendors of malfeasance ranging from

[35] S. 5355, 2013 Reg. Sess. (N.Y. 2013), http://open.nysenate.gov/legislation/bill/S5355-2013.
[36] H.R. 946, 2014 Reg. Sess. (La 2014), https://www.legis.la.gov/legis/BillInfo.aspx?i=224975.
[37] H.R. 1989, 54th Leg., Reg. Sess. (Okla. 2013), http://webserver1.lsb.state.ok.us/cf_pdf/2013-14%20ENR/hB/HB1989%20ENR.PDF.
[38] S. 1177, 2014 Reg. Sess. (Cal. 2014), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_bill_20140220_introduced.pdf.
[39] *See* Benjamin Herold, *Legislative-Advocacy Group's Model Bill Tackles Privacy of Student Data*, EDUC. WK. (Dec. 3, 2013), http://www.edweek.org/ew/articles/2013/12/03/14alec.h33.html.

selling children's data to downright identity theft.[40] Yet, entrenching behind a "no vendor" model is no panacea, as schools are unlikely to have the capabilities to carry the technological load. In fact, schools often turn to vendors as the most secure avenue for the safeguarding of student data. Instead, schools must put in place appropriate data governance mechanisms to actively manage their information systems and relationships with vendors. This includes, but is not restricted to, making sure there is appropriate language in vendor contracts to comply with existing legal obligations.

Privacy laws typically do not limit the sharing of personal information with vendors, so long as the vendor acts under instructions and control of the first party. Without a concept of agency, privacy law would effectively compel first parties to develop in-house expertise to fulfill every aspect of their activities. Hospitals, for examples, would need to establish functions to specialize in accounting, law, interior design, dining, cleaning, recreation, and more. Entire departments would be required to manage information technologies, data security, software and online services.

Such tasks have become daunting for even the largest technology companies.[41] For example, leading online companies such as LinkedIn and Expedia, software providers such as Adobe and SAP, information processors such as Thomson Reuters, and system integrators such as Nokia – all use Amazon Web Services for satisfying multiple IT functions.[42] Reliance on vendors including cloud providers, IT consultants, transaction processors, and other business associates has become the industry norm.[43] Schools too need to engage a variety of experts to handle a broad range of tasks, and such relationships inevitably entail sharing students' data.

Some have proposed relying on parental consent as a solution for placing data in the cloud or enabling use of certain technologies. Certainly parents should be part of the technology planning process at schools and school districts through appropriate committees and consultation. But individual parents are ill placed to become independent technology auditors making procurement or policy choices for their children's schools. Asking parents to consider and examine the details of technical infrastructure is more likely to overwhelm parents than advance student privacy. Joel Reidenberg, who has been critical of school data use, argued that providing opt-out mechanisms would 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."[44] In addition, accommodating the technology choices of individual parents would force schools to operate

---

[40] *See* Diane Ravitch, *Is inBloom Engaged in Identity Theft?*, DIANE RAVITCH'S BLOG (Apr. 7, 2013), http://dianeravitch.net/2013/04/07/is-inbloom-engaged-in-identity-theft/.

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

[41] *See Customer Success. Powered by the AWS Cloud*, AMAZON WEB SERVICES, https://aws.amazon.com/solutions/case-studies/?nc1=f_cc (last visited May 6, 2014).

[42] *See Customer Success. Powered by the AWS Cloud*, AMAZON WEB SERVICES, https://aws.amazon.com/solutions/case-studies/?nc1=f_cc (last visited May 6, 2014).

[43] *See* Jan Hertzberg, *Managing Data Security and Privacy Risk of Third-Party Vendors*, GRANT THORTON (Oct. 15, 2011), http://www.grantthornton.com/staticfiles/GTCom/Health%20care%20organizations/HC%20-%20managing%20data%20-%20FINAL.pdf.

[44] Joel Reidenberg, *Education Data: Privacy Backlash Begins*, FORDHAM UNIV. NEWSROOM (Apr. 26, 2013), http://law.fordham.edu/29764.htm.

multiple duplicative systems, an impossible task that would also leave some children without access to basic services that others receive, raising equity concerns.

Information privacy laws have traditionally carved out a category of trusted third parties, who could under certain restrictions obtain data from first parties. The European Data Protection Directive distinguishes between "data controllers," who determine the purposes and means of data use, and "data processors," who operate at their behest.[45] While data controllers are subject to the full gamut of privacy laws, including the principles of transparency, individual choice, subject access, and data minimization, processors are mainly required to adhere to purpose limitation clauses and implement appropriate data security. In the United Kingdom, for example, the Information Commissioner's Office specifically defines third parties in such a way to ensure that any vendor authorized to process data on a first party's behalf "is not considered a third party."[46]

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule applies to protected health information (PHI) possessed by "covered entities," which include "health plans, health care clearinghouses, and health care providers."[47] However, HIPAA recognizes that covered entities cannot conduct all of their functions and activities themselves. It therefore permits covered entities to disclose PHI to "business associates,"[48] for purposes such as claims processing, quality assurance, billing, and data analysis or administration and more.[49]

PHI can only be disclosed to a business associate if a covered entity "obtain[s] 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."[50] Furthermore, any disclosed information may not be used for the business associate's independent use or purposes.[51] Health providers can only disclose information to help themselves carry out their essential health care functions. As additional protection, business associates who violate HIPAA are subject to the same punishments as covered entities.

---

[45] Council Directive 95/46, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, arts. 2(d)-(e), 1995 O.J. (L 281) 31, 38; *see also* Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor" at 12, 00264/10/EN/WP 169 (Feb. 16, 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[46] *Key Definitions of the Data Protection Act*, ICO, http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions (last visited May 6, 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." *Id.*

[47] *See* 45 C.F.R. § 160.102. Protected health information (PHI) under HIPAA consists of all "individually identifiable health information." 45 C.F.R. § 160.103.

[48] *See* 45 C.F.R. § 164.502.

[49] 45 C.F.R. § 160.103.

[50] U.S. Dep't of Health & Human Serv., *Business Associates*, HHS.GOV, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last revised Apr. 3, 2003).

[51] *See id.*

The Gramm-Leach-Bliley Financial Modernization Act (GLBA) of 1999 protects the privacy of consumer financial information held by "financial institutions." Under GLBA, consumers are entitled to opt-out of banks or other financial institutions sharing information with nonaffiliated third parties.[52] However, financial institutions are authorized to share data with service providers operating to perform services for the financial institution or to function on its behalf, including marketing the bank's own products or services. In these cases, financial institutions are required to provide consumers with notice of the arrangement and contractually prohibit the third party from disclosing or otherwise using the information.

Hence, U.S. and global information privacy laws recognize the need to allow third-party vendors controlled access to data. Such vendors are typically tasked with data security and use restrictions, while customers retain data governance obligations, including the scoping of data collection, storage and use. Letting individuals opt-out of having their information shared with vendors would render it difficult for organizations, including health care providers, financial institutions and schools, to fulfill their basic responsibilities toward their patients, clients and students.

Similar to HIPAA, GLBA and the EU Directive, FERPA recognizes data sharing with "other school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests."[53] To be considered a "school official," a vendor must perform an institutional function for which the school would otherwise use its own employees; meet the criteria for being a school official with a "legitimate educational interest" as set forth in the school's or district's annual FERPA notification; be under the "direct control" of the school or district with respect to the use and maintenance of education record; and use any student information only for authorized purposes and not re-disclose information from educational records to any other party. [54] Hence, merely identifying an entity as a "school official" does not provide it with *carte blanche* access to or use of education records.[55]

School officials include contractors, consultants, and even volunteers to whom a school has outsourced institutional services or functions.[56] As a result, vendors such as school tutors, cafeteria and busing services, attorneys and information technology providers are classified school officials. While confusing in terms of terminology, the school official exemption provides flexibility and legal grounding for schools to share data with vendors, so long as such vendors act under school control and use data strictly for designated educational purposes. Indeed, until the FERPA amendments in 2008, it was not clear that vendors could be designated "school officials," creating a roadblock for many of the services that are now commonplace.

---

[52] *See Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information*, FDIC Compliance Manual VIII 1.2 (Jan. 2014), *available at* http://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf.
[53] 20 U.S.C. § 1232g(b)(1) (Supp. II 2002). Certain restricted types of data sharing could conceivably be authorized under FERPA's "directory information" provisions. However, the purview of these provisions is limited in the context of enabling vendor activity, as vendors are not provided with data under the directory information exception.
[54] 34 CFR § 99.31(a)(1)(i).
[55] *See Defining "Legitimate Educational Interests"*, NAT'L CTR. FOR EDUC. STATS, http://nces.ed.gov/pubs2004/privacy/section_4b.asp (last visited May 6, 2014).
[56] *See id.*

The U.S. Department of Education recognizes the necessity to employ vendors to provide technology services. In its recent guidance on online education services, it notes: "Some types of online educational services do use FERPA-protected information. For example, a district may decide to use an online system to allow students (and their parents) to log in and access class materials. In order to create student accounts, the district or school will likely need to give the provider the students' names and contact information from the students' education records, which are protected by FERPA."[57] At the same time, the Department of Education clarifies that "when a school or district discloses or re-discloses FERPA-protected data to contract out for certain services, its contractor never 'owns' the data, and can only act at the discretion of the disclosing entity and in compliance with the FERPA."[58]

The preamble to the 2008 FERPA amendments explains:

> "Exercising direct control could prove more challenging in some situations than in others. Schools outsourcing information technology services, such as web-based and e-mail services, should make clear in their service agreements or contracts that the outside party may not use or allow access to personally identifiable information from education records, except in accordance with the requirements established by the educational agency or institution that discloses the information."[59]

Despite fact that many types of tech vendors now qualify as school officials under the FERPA, privacy concerns about their services abound and have become a major source of contention. Specifically, critics have raised concerns about vendors' poor contractual commitments, lax security practices, and potential use of data for non-educated related purposes, including marketing.

Security

The sharing of schools' student data with third party vendors and eventual migration from local servers to the cloud inevitably raises concerns about privacy and data security. It is certainly essential that vendors that service schools provide first class security for any student data they hold. Both FERPA and COPPA impose data security obligations as does the Federal Trade Commission's ("FTC") emerging "unfairness" doctrine under Section 5 of the FTC Act.

Some have expressed concern that cloud services by their nature create security risks. Data migrates from multiple schools via the web to reside in a tech vendor's vault, which is accessible by multiple parties. One commentator warned against outsourcing to companies that "are the

---

[57] PRIVACY TECHNICAL ASSISTANCE CTR., U.S. DEP'T OF EDUC., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES (Feb. 2014), *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf.

[58] Letter from Arne Duncan, Sec'y of Educ., to Sen. Edward Markey, (Jan. 13, 2014), http://www.markey.senate.gov/imo/media/doc/2014-01-10_Education_Privacy.pdf.

[59] 73 Fed. Reg. 74,805, 74,816 (Dec. 9, 2008).

subject of 20-year consent decrees for engaging in deceptive practices surrounding privacy and/or security."[60] According to a comprehensive research into schools' cloud computing practices recently conducted by the Fordham School of Law's Center on Law and Information Policy (CLIP Study), cloud vendor contracts often fail to impose security breach notification obligations or data deletion requirements, which are in fact mandated [for schools] under FERPA.[61] The research study states that "[s]chool district cloud service agreements generally do not provide for data security and even allow vendors to retain student information in perpetuity with alarming frequency."[62]While these are concerns, it is also important to recognize that vendors often address these issues in their privacy policies. It is also important to recognize that the absence of explicit contractual language may permit an activity to happen, but it does not mean that activity is happening and that the vendor is not otherwise required to follow existing laws including FERPA, COPPA, and the Protection of Pupil Rights Amendment (PPRA) as well as broader federal and state data breach laws.

Yet as most Fortune 500 companies holding sensitive financial or health data have determined, it is typically safer to rely on the security practices of vendors who can deploy hundreds of staff and first class encryption tools than to develop those same capabilities in house. Schools or even large school districts would be hard pressed to keep up with continuous alerts, security patches and updates needed to maintain systems secure. In addition, critics who argue that the alternative to cloud storage or email services is a school hosted system often ignore the fact that most schools already rely on remote servers for computing powers.

The FTC has recently stressed the importance of exerting appropriate controls over vendors' data security practices in the matter of GMR Transcription Services, Inc.[63] While not in the context of education, the GMR case illustrates the FTC's approach toward failures in contracting between a company and its data service provider. The FTC complaint alleged that GMR failed to "require [vendor] by contract to adopt and implement appropriate security measures to protect personal information in medical audio and transcript files, such as by requiring that files be securely stored and securely transmitted to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files; take adequate measures to monitor and assess whether [vendor] employed measures to appropriately protect personal information under the circumstances." Moreover, the FTC faulted GMR for not doing due diligence before hiring its data service providers.

While the GMR case demonstrates the FTC's approach toward vendors' security obligations, it may be difficult to impose FTC security standards on vendors who hold data for schools without

---

[60] *See* Chris Hoofnagle, *The Good, Not So Good, and Long View on Bmail*, BERKELEY BLOG (Mar. 6, 2013), http://blogs.berkeley.edu/2013/03/06/the-good-not-so-good-and-long-view-on-google-mail/.

[61] Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, Fordham Ctr. L. & Info. Pol'y, 31-32, (Dec. 2013) [hereinafter "CLIP Study"], *available at* http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip. For deletion obligations, *see, e.g.*, 20 U.S.C. §§ 1232g(b)(1)(F), (b)(3).

[62] CLIP Study, *supra* note 61.

[63] Press Release, *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, FED. TRADE COMM'N (Jan. 31, 2014), http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

making any direct representation to individual users of their service. One area where state legislation may be useful is requiring vendors to schools to provide appropriate security protections to the data they hold regardless of the existence of a user interface.

Contracting

School systems (FERPA contracts)

When a school shares student data with a technology vendor, the privacy and data security obligations of the vendor must be established. FERPA requires that PII from educational records shared with a vendor must remain "under the direct control of the school or district with regard to the use and maintenance of education records."[64] This is most often accomplished through a contract with terms that, establish a FERPA basis for disclosure of personal information and limit uses and re-disclosures of personal information. They should also include security requirements, security breach obligations and indemnification and liability provisions. Alas, according to the CLIP Study, the contracts of schools with service providers are lacking.[65]

The CLIP Study states, "Districts frequently surrender control of student information when using cloud services: fewer than 25% of the agreements specify the purpose for disclosures of student information, fewer than 7% of the contracts restrict the sale or marketing of student information by vendors, and many agreements allow vendors to change the terms without notice."[66] In addition, "An overwhelming majority of cloud service contracts do not address parental notice, consent, or access to student information."[67] The report concludes that "with respect to data control, the districts' agreements do not generally assure compliance with FERPA."[68] These findings imply violations of the spirit and letter of FERPA as well as other children's privacy laws.[69] [70]

An additional complication arises when schools or teachers execute agreements with technology vendors via click-wrap. Indeed, most consumer transactions in online and mobile environments are entered into via click-wrap. Typically, neither schools and teachers nor small technology vendors have the incentive to negotiate such contracts, which sometimes do not explicitly provide FERPA commitments and may allow vendors to unilaterally change the terms of the deal. The

---

[64] 34 C.F.R. § 99.31(a)(1)(i)(2). The Department of Education explains, "While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider." PRIVACY TECHNICAL ASSISTANCE CTR., *supra* note 57.

[65] CLIP Study, *supra* note 61.

[66] *Id.*

[67] *Id.*

[68] *Id.* at 28.

[69] Other findings include that "only thirty-three percent (33%) of the agreements gave districts the right to audit and inspect the vendor's practices with respect to the transferred data" and "only one-third contained provisions that prohibit or limit the re-disclosure of student data or other confidential information." *Id.*

[70] However, it should be noted that FERPA does not explicitly require that all of these terms be included in contracts, such that some might be included in privacy policies. It should also be noted that, while many of these items should ideally be in contracts, their lack of inclusion is not evidence that vendors are acting inappropriately in their use and sharing of the data as school service providers are aware that they are restricted in their use and sharing of PII to the intended educational purposes.

Department of Education stresses that "[e]xtra caution and extra steps are warranted before employing click-wrap consumer apps." Contracting practices that are not fixed would not seem to comply with existing laws and regulations for direct control, including the Department of Education requirements and best practices.[71] This does not imply, of course, that click-wrap is inherently deficient; rather the point is that when used in the education arena, click-wrap contracts need to transparently and satisfactorily address at least the minimum requirements of applicable education privacy laws.

To be sure, when working with technology vendors, schools cannot be allowed to abdicate their responsibilities toward students' privacy. Kathleen Styles, the chief privacy officer of the Department of Education, explains that "districts are responsible for the protection of their data, regardless of where they are stored. It doesn't matter whether the records are located in a locked file cabinet, in a server on the school premises, or on a server in the cloud."[72] But vendors designing and marketing their services for use in schools too must bear some of the costs of adapting their business models to the school environment. National vendors are often more likely than local schools or school districts to have the wherewithal to craft FERPA-compliant contracts. This, in particular, is the case where the technology architecture has become so complicated that no one outside of the tech vendor's organization is likely to have a firm grasp of the inner workings of the system concerned.

In sectors where they provide a one-size-fit-all contractual template, vendors often disclaim responsibility for customers' legal obligations. Yet such an approach is ill-suited for serving education institutions, given the disparity in legal resources and expertise. The typical inertia leading vendors to serially reuse existing boilerplate in transactions with different customers regardless of the business sector served must change to take account of the unique sensitivities of student data.

The imperative to adapt cloud contracts to the needs of a regulated sector is not new. Much like schools have to comply with FERPA obligations, the federal government has had to overcome obstacles in order to contract outsourcing solutions to the cloud. In order to streamline contracting processes and set forth standard criteria for engaging vendors, the U.S. CIO initiated an on-ramp process, the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[73] Other regulated industries, including health care and finance, have worked to adapt contracting practices to accommodate cloud solutions. Google, for example, has recently announced it would support HIPAA-compliant clouds, with Google Apps and Google Cloud Platform entering into business

[71] *See also* PRIVACY TECHNICAL ASSISTANCE CTR., U.S. DEP'T OF EDUC., WRITTEN AGREEMENT CHECKLIST (updated May 2013), *available at* http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf; PRIVACY TECHNICAL ASSISTANCE CTR., U.S. DEP'T OF EDUC., DATA BREACH RESPONSE CHECKLIST (Sept. 2012), *available at* http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf.

[72] Daniel Solove, *Interview with Kathleen Styles*, *supra* note 13.

[73] *FedRAMP*, CLOUD CIO.GOV, http://cloud.cio.gov/fedramp (last visited May 6, 2014).

associate agreements to handle HIPAA-protected information on behalf of a range of healthcare applications and technologies.[74]

Similar solutions can be crafted to modify existing cloud business models to the market for education. Some of this is already happening, with businesses such as Google and Microsoft offering ad-less versions of existing product suites, including Google Apps for Education, Office 365 for Education and Bing. Much more work still needs to be done; and the process is unlikely to be as streamlined as the federal on-ramp program, given the distributed nature of the education system, which is scattered across states, school districts and stand-alone schools.

Individuals (COPPA contracts)

Not only schools, but also teachers, parents, and students introduce ed tech into classrooms. Such is the case when a student downloads an app recommended by his teacher; creates a cool program for use by his friends; or just watches a video on YouTube where an expert explains how to solve a math problem. In cases where companies collect data directly from students, COPPA applies to protect information gleaned from the under 13 year old audience. Here, the legal attention devoted to FERPA compliance by companies or schools varies widely. On the one hand, some schools provide approved software lists to teachers, and vendors design products specifically for school use. On the other hand, some schools do not think twice about the privacy issues involved with providing "free" services.

Specifically, under COPPA, any website directed at children or knowingly collecting personal information from children under 13, must provide parental notice and obtain consent. Although schools may provide consent on behalf of parents, the mechanics and scope of such consent have not been clear. Acting to clarify this issue, the FTC updated its COPPA guidance in in April 2014. The FTC notes that "under the school's ability to consent on behalf of the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose…. because the scope of the school's authority to act on behalf of the parent is limited to the school context."[75] Significantly, the FTC clarified that school consent cannot substitute a parent's "in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service."[76]

In addition, in language recently introduced in the April 2014 guidance, the FTC states that the "operator's method [of obtaining consent] must be reasonably calculated, in light of available technology, to ensure that a school is actually providing consent, and not a child pretending to be

---

[74] *See* Matthew O'Connor, *Google Cloud Platform Provides Support for HIPAA Covered Entities*, GOOGLE CLOUD PLATFORM BLOG (Feb. 5, 2014), http://googlecloudplatform.blogspot.com/2014/02/google-cloud-platform-provides-support-for-hipaa-covered-entities.html.

[75] *See Complying with COPPA: Frequently Asked Questions*, Bureau of Consumer Protection Business Ctr., http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions#Schools (last visited May 6, 2014).

[76] *Id.*

a teacher, for example."[77] How operators will verify that they are dealing with a school official remains unclear. It has been difficult enough to operationalize parental verification requirements under COPPA; verifying the identity of a teacher and his or her authority to act in the name of a school appears daunting. It is noteworthy that many operators serving students in schools opt for gaining explicit parental consent, rather than relying on schools for that consent. This consent is often coordinated through the school, but the actual consent comes directly from the parent to the operator.

Interestingly, the FTC suggests that "as a best practice," it will be schools or school districts and *not individual teachers* who should ideally decide whether to engage a particular vendor's site or service. The best practice apparently aims to ensure appropriate vetting, which a teacher may not have the expertise or time to do themselves. As an additional, "best practice," the FTC proposes that "the school should consider providing parents with a notice of the websites and online services whose collection it has consented to on behalf of the parent."[78] The overall effect of this guidance is that a teacher who identifies an online resource or an app they wish to use for a lesson would not do so unless the operator has been pre-approved. Indeed many school districts are setting up lists of apps or programs that they have reviewed for privacy compliance (e.g., for example the Houston school district software rating for parents).[79] Others may simply ignore or not be aware of this limitation and continue to use the tools they deem most useful for their classroom.

Current COPPA practice has led many vendors to declare that their products are intended solely for individuals over 13 years of age, to avoid having to navigate the treacherous waters of the parental verification process. Regrettably, parents find themselves helping their children lie about their age to facilitate their use of leading email services, social networks, video sites and app stores. At the end of the day, in its current incarnation, COPPA is failing at blocking the access of determined children and youths to desired web services. Instead, it unwittingly serves as a deterrent for general web services from providing more privacy friendly versions of their services to children.

By making parental and teacher verification more practical, COPPA could incentivize a wide swath of vendors to provide ad free and safer versions of their products and ensure their availability in the school market. Today, many web services are barred in schools although it is an open secret that students regularly use them at home. And while the FTC has taken steps in this direction by allowing safe harbor programs to approve new age verification technologies as well as by approving new methods directly, it continues to limit some of the most widely used age verification mechanisms, such as the use of credit card verified app store accounts. The FTC's concern has been that parents share their app store passwords with their children. Yet a study conducted by the Future of Privacy Forum showed that 72% of parents have never shared this information with

[77] *Id.*
[78] *Id.*
[79] *Software Ratings for Parents*, HOUSTON INDP'T SCHOOL DIST., http://www.houstonisd.org/Page/109830 (last updated May 5, 2014).

their children (age 3-12), and only 4% did not require children to ask permission before purchasing or downloading free apps.[80]

Commercial Use

The debate over commercial activities in schools is decades old.[81] Schools have long had policies to determine the contours of legitimate commercial activities ranging from billboards in sports fields, vending machines in cafeterias and outsourced yearbooks, to ads and branding on textbooks and core education products. This ongoing debate is now converging with the heated discussion surrounding commercial use of student data.

According to a January 2014 survey by Common Sense Media, 86 percent of adult respondents agreed that "oversight is necessary to ensure [children's] private information is not exploited for commercial purposes and stays out of the hands of the wrong people."[82] Services such as email and document sharing that are offered to educational institutions for free automatically flag privacy and data security concerns, creating perceptions that if the service is free then the business model must be to monetize the data, whether or not that is actually true. Massive Open Online Courses (MOOCs) have also come under close scrutiny for existing or potential future data monetization.[83] Significantly, the public maelstrom around inBloom featured allegations that the initiative was "a new experiment in centralizing massive metadata on children to share with vendors, and then the vendors will profit by marketing their learning products, their apps, their curriculum materials, their video games, back to our kids."[84] In reality, the model did allow for data to be shared with vendors, but largely at the discretion of school districts to streamline their ability to integrate third-party applications of their choosing.

U.S. Senator Ed Markey has recently announced plans to introduce legislation mandating that student information "never be used to market products to children."[85] And under the California state senate's proposed Student Online Personal Information Protection Act (SOPIPA), the use of "a student's personal information for any commercial purpose, including, but not limited to advertising or profiling" is prohibited.

---

[80] *New Survey on App Stores and Account Info Sharing – What This Means for COPPA*, FUTURE OF PRIVACY FORUM (Sept. 6, 2013), http://www.futureofprivacy.org/2013/09/06/new-survey-on-app-stores-and-account-info-sharing-what-this-means-for-coppa/.

[81] *See* ALEX MOLNAR ET AL., NAT'L EDUC. POLICY CTR., SCHOOLHOUSE COMMERCIALISM LEAVES POLICYMAKERS BEHIND – THE SIXTEENTH ANNUAL REPORT ON SCHOOLHOUSE COMMERCIALIZING TRENDS: 2012-2013, *available at* http://nepc.colorado.edu/files/trends-2013.pdf.

[82] *Student Privacy Survey*, COMMON SENSE MEDIA, http://cdn2-d7.ec.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf (last visited May 6, 2014).

[83] *See* Mark Edmundson, *The Trouble with Online Education*, N.Y. Times (July 19, 2012), http://www.nytimes.com/2012/07/20/opinion/the-trouble-with-online-education.html; *see* Audrey Watters, *Student Data Is the New Oil: MOOCs, Metaphor, and Money*, HACK EDUCATION (Oct. 17, 2013), http://www.hackeducation.com/2013/10/17/student-data-is-the-new-oil/.

[84] Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html.

[85] David Nagel, *Student Data Not a 'Product' to Be 'Sold to the Highest Bidder'*, TRANSFORMING EDUC. THROUGH TECH. J. (JAN. 14, 2014), http://thejournal.com/articles/2014/01/14/student-data-not-a-product-to-be-sold-to-the-highest-bidder.aspx.

The Market

To facilitate a levelheaded policy discussion, the highly charged concept of commercialization in schools needs to be unpacked.

First, schools have long exposed students to non-data related commercial activity; for example, by placing billboards or branding merchandise in school cafeterias or playing fields or serving generalized, non-targeted ads on an online school newspaper or yearbook. Such commercial activities have long been the purview of local schools or school districts, which had the autonomy to determine where and how to earn revenue or recognize local sponsors. Although these practices may be restricted as a result of anti-marketing sentiments, they often implicate neither student privacy nor information privacy laws.[86]

Second, vendors may use student information to enhance and improve existing products and services and develop related products and services; and this may entail improving the same products and services sold to the students' schools, improving other education products and services, or other non-education products and services. FERPA would bar use of student records for purposes that are not relevant to the schools served, but other non-covered student data could be used to improve a vendor's other services. As such, it is important to keep in mind the two dimensions of the issue – the type of data, and the use of that data. This issue remains contentious given that some vendors have a broad sweep of activities that are unrelated to the services they offer schools. Some proposed state bills would prohibit uses for both educational and non-educational purposes, regardless of the type of data, to the consternation of vendors who believe that commercial activity in this vein is both appropriate and necessary to serve their education customers.

Third, vendors may use students' information to "market" or "advertise" to them, their family, or their teacher new education products or services (for example, by recommending a level two math app after a student completes level one). This area too remains a subject of intense debate. This scenario requires perhaps the most unpacking as the opportunities to customize learning intersect with concerns around commercial activity. Some argue that students and families are using many third-party technologies at home but without sufficient connection to school activities, and so recommendation engines provide opportunity to empower families with information they can use to more effectively help their children outside of school. There is also the question of helping educators identify resources from the primary vendor or vendor partners that meet their student or school needs. Finally, the appropriate use issue intersects with issues around the type of data and access to data. For example, some models do not require access to or sharing of personal

[86] In this respect, SOPIPA is anomalous, attempting to prohibit not only data driven marketing but also mandating that a website used by K-12 students "shall not allow, facilitate, or aid in the marketing or advertising of a product or service to a K–12 student on the site, service, or application." S. 1177, 2014 Reg. Sess. (Cal. 2014), http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_bill_20140220_introduced.pdf. As such, it prohibits general-audience or contextual advertising that does depend on any student information, whether personal or not.

information, but instead recommendation engines are based on meta-data that match up student needs with resources that work best "for students like you."

Fourth, and of greatest concern, is the prospect of vendors targeting students with personalized ads unrelated to the educational purpose, or selling their information to third parties. There is wide agreement that these uses are most clearly inappropriate. While such practices would in most cases violate FERPA and COPPA, critics argue that statutory restrictions contain loopholes, which could enable, for example, transactions in information deemed not personal, or use of children's data once they cross the COPPA threshold of age 13.

Finally, some critics are more generally concerned about the growing role of business in education. Companies that once sold textbooks and testing are now spearheading a sprawling industry of learning, where they provide not only the means of delivery but also curriculum and test development. Other critics disdain the corporate and foundation based education reformers, who, they argue, advance a data and performance-driven agenda. The concern is that rather than supporting smaller class sizes and better paid teachers, elites such as the Gates and Walton foundations are advancing ideas linked to measurement, testing and performance. In MOOCs like Coursera and Udacity, for example, vendors have themselves become the education institutions, threatening the business model of traditional non-profit schools. With the K12 education system provided primarily today by unionized teachers in the public sector, new educational models are the source of heated opposition.

Most stakeholders would agree that leveraging student information from a school-procured system to drive non-educational behavioral advertising at home would be inappropriate. But the line blurs quickly. Activities that could be considered commercial behavioral advertising by some would be viewed as part of the adaptive learning experience by others. This includes recommending apps or content to teachers, parents or students based on student performance, or offering additional features to a subscription service to improve student outcomes. For example, should a developer of a math app be authorized to offer students who perform well an advanced math app? Should an education social network such as Edmodo be permitted to feature a third party app store for kids? And could such an app store be tailored to third grader as opposed to offering a generic collection of apps? If an education service detects a security vulnerability on a website offered to a school, should it be able to leverage its knowledge to protect information in transactions with other school or even non-school clients? And what about using the data to develop software offered to the general market?

Even with the best of intentions, the crossover of commercial vendors, products and apps into the field of education can spawn awkward moments and raise thorny policy questions. Many online and mobile services are offered through a "freemium" model, requiring no payment upfront but proposing upsells or serving ads to users. For example, Microsoft's Bing for Schools was designed for use in a K-12 environment and therefore does not feature advertisements, refrains from mining users' search queries, and automatically filters out adult content. But the Bing Rewards program incentivizes students to search with Bing by rewarding their schools free Surface tablets, arguably

a commercial practice.[87] Google Apps for Education has been criticized by SafeGov[88] for scanning and analyzing the content of student email and web interactions although it does not serve students with ads.[89] Google has now confirmed that it has ended this practice.[90]

Numerous websites that provide education services serve cookies, including third party cookies which could ostensibly be used to profile users. Khan Academy, a leading resource for educational content and Edmodo, a leading learning management system for teachers, both had to scramble to explain that they did not sell student information, after their policies came under scrutiny. *Education Week* reported that "a review of each group's privacy policies …. yielded concerns about the use of tracking and surveillance technologies that allow third parties to gather information on students; questions about the collection, use, and sharing of massive amounts of student 'metadata'; and criticism of the growing burden on students and families, who experts maintain are being forced to navigate an ever-shifting maze of dense vendor policies on their own."[91] Obviously, even with the best of intentions, market players are struggling to get it right.

Legislative Gaps

The patchwork of United States privacy laws generally, and education privacy laws in particular, is laden with gaps. The provision of education services by for-profit entities operating outside the purview of education privacy laws raises challenging and novel privacy questions. For example, MOOCs, when they are not part of federally funded education agencies or institutions, are not subject to FERPA, PPRA or COPPA (unless they enroll children under 13). To emphasize this point, Coursera, for example, includes in its terms of use a "Disclaimer of Student-University Relationship", stating: "You agree and acknowledge that nothing in these Terms of Use … establishes any relationship between you and any university or other educational institution with which Coursera may be affiliated…"[92] Other providers operating in this space are cautious with respect to the nomenclature they use, for example, to designate "certificates" earned by "participants" as opposed to "degrees" awarded to "students".

Additional loopholes may weaken protection even within the scope of existing legislation. For example, under FERPA, de-identified data may be shared without consent with any party for any purpose, arguably including behavioral advertising.[93] And while the Department of Education

[87] *See* John Ribeiro, *Microsoft Opens Ad-Free Bing for Schools Search Engine to All U.S. Schools*, PCWORLD (Apr. 23, 2014), http://www.pcworld.com/article/2147200/bing-for-schools-out-of-pilot-stage-promises-adfree-search.html.
[88] *Partners*, SAFEGOV, http://safegov.org/partners (last visited May 5, 2014).
[89] *See* Jeff Gould, *Google Admits Data Mining Student Emails in Its Free Education Apps*, SAFEGOV (Jan. 31, 2014), http://safegov.org/2014/1/31/google-admits-data-mining-student-emails-in-its-free-education-apps.
[90] *See* Juan Carlos Perez, *Google Stops Scanning Gmail Messages for Ads in Apps for Education*, PCWORLD (Apr. 30, 2014), http://www.pcworld.com/article/2149960/google-stops-scanning-gmail-messages-for-ads-in-apps-for-education.html.
[91] Benjamin Herold, *Prominent Ed-Tech Players' Data-Privacy Policies Attract Scrutiny*, EDUC. WK. (Apr. 14, 2014), http://www.edweek.org/ew/articles/2014/04/16/28privacy_ep.h33.html.
[92] *Terms of Use*, Coursera, https://www.coursera.org/about/terms (last revision Jan. 2, 2014).
[93] 34 C.F.R. §99.30.

issued sophisticated guidance with respect to de-identification,[94] critics argue that as long as it is not irreversibly anonymized, de-identified information continues to harbor privacy risks. In addition, as previously noted, COPPA does not restrict the collection of data about children over the age of 13, leaving out most high school students.

A PATH FORWARD

Some of the privacy issues arising in the field of education reflect similar concerns in other contexts such as healthcare, financial services and e-government. They result from the application of new technology on top of long-held views and traditions. And they result in part from laws originating in the 1970s to a new techno-social reality. Contractual and data security arrangements with vendors must be tightened, as school information routinely migrates to the cloud. Decisions must be reached concerning the scope of legitimate uses of student data, including the degree those decisions should be made by parents, localities, state governments or nationally. Clearly, personal student data should not be sold or used for behavioral ads; but can vendors harness it to improve products and services within or outside the education space? And may vendors market education related products to students, families and educators based on their previous interactions? Key terms, such as "education records" and "personally identifiable information" should be clarified. Lines need to be drawn in the sand with respect to de-identification. These issues involving privacy in education are similar to those faced by consumers, professionals, policymakers and privacy professionals in every sector of society.

More difficult questions concern the desirable role of technology and data in the field of education. Numerous parties view this as a high stakes affair, with parents worried about their children, teachers about jobs and school environment, school administrators about performance and cost efficiency, states about funding, and the federal government about the future of the nation. Heated debates will continue and revolve around the ethics of data use and the policy of education more than the technicalities of outsourcing contracts and data security obligations.

Engendering Trust

The goal of both school leaders and their vendors should be to empower parents and students and teachers and bring them along for the technology ride. Particularly in the field of education, an adversarial relationship between customers and vendors is toxic. If vendors are regarded as being motivated to misuse or sell student information rather than serving their users with the highest quality educational services, there is little hope for ed tech. If, however, trust can be engendered between all relevant stakeholders, the discussion can pivot to maximizing big data benefits while restricting privacy and civil liberty costs.

At this point, trust may not be established simply by better contracting practices[95] or even through compliance with the technicalities of FERPA and PPRA. Parents, students and teachers who do

[94] PRIVACY TECHNICAL ASSISTANCE CTR., U.S. DEP'T OF EDUC., DATA DE-IDENTIFICATION: AN OVERVIEW OF BASIC TERMS (updated May 2013), *available at* http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf.
[95] CLIP Study, *supra* note 61**Error! Bookmark not defined.**.

not read, much less understand, vendor contracts, will likely not be satisfied simply by an additional contract clause. 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."[96] Instead, trust must be built by enhanced transparency into *data practices not into data contracts*, demonstrating to parents, students and teachers the benefits and promise of data use and assuaging the fears of abuse and student commodification.

Parents are eager to reap the rewards of big data by enabling a more interactive, challenging, individually tailored and dynamic education experience for their children. A recent set of parent focus groups by the Data Quality Campaign found that parents were most interested in the equity of access to information about their students, teachers and schools. They want to have meaningful access to information about their children, to see how they are doing in real time, to nurture their strengths and support them in their weaknesses. They are not interested in technologies that stand to improve only school or state reporting systems. Consequently, they should be granted access to students' data in a usable format, as well as insight into the logic underlying the algorithms used to assess their performance.

Data Featurization

We have previously argued for a need to "featurize" data and enhance the transparency of algorithms. These same concepts are key in the education sphere. Parents need to see the value of data to buy into the ed tech revolution. Data featurization includes dashboards for parents, not just school officials, providing them access to their children's data. Currently the only "dashboard" most parents have is a quarterly report card, which leaves them poring over grades and comments and hungry for more. Parents should benefit from access to data before the end of quarter; they should be able to see the inner components of each grade; to understand where their child struggles, where he excels, and where his excellence is off the chart calling for more challenges and growth opportunities. And while FERPA already requires parent access, this right is rudimentary and therefore not meaningfully exercised. Schools and vendors should seek to ensure that parents and students can access and use student data in a meaningful way, transfer it with them if a student moves, and analyze and study the information on their own or with the help of their own experts or third party tools.

In many ways, the featurization idea is captured by existing proposals for "digital backpacks" that would allow students to download their data in a usable format to a portable digital vault. Similar to the blue button for personal health records or the green button for smart metering information,[97] a digital backpack can provide parents with confidence that data is not only used to assess and rate their children's performance but also as an additional tool to help them ensure their children's needs are met. Experiencing firsthand the nature and value of information will help alleviate

[96] 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), http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[97] EXEC. OFFICE OF THE PRESIDENT, *supra* note 2, at 14.

parents' privacy concerns as well. Despite the promise, implementation of such technologies have been very limited to date [98]

Algorithm Transparency

In *Big Data For All: Privacy And User Control In The Age Of Analytics*, we explained that in a world of big data, transparency must extend beyond simple access to raw information to provide insight into the inner working of the machine. We wrote, "[t]o minimize concerns of untoward data usage, organizations should disclose the logic underlying their decision-making processes to the extent possible without compromising their trade secrets or intellectual property rights."[99] We explained that "[i]t is imperative that individuals have insight into the decisional criteria of organizations lest they face a Kafkaesque machinery that manipulates lives based on opaque justifications."

At a time when concerns about new types of discrimination are stoked by big data practices, stakeholders must understand how and to what effect student data is being used. To be effectively and rationally resolved, privacy concerns should first be disentangled from policy debates over education reform and the outcomes of data use. Conversely, kneejerk responses may end up exacerbating instead of solving privacy problems. For example, New York's legislative swipe at inBloom, which effectively put the nonprofit service provider out of business, will not restrict an identical service from operating in the state as long as it contracts with each individual regional board of education rather than with the state as a whole (arguably weakening any leverage that education institutions have in their negotiations with national vendors). Hence, even as the legislature sought to address the political concerns raised by inBloom, it left the state with irrational limitations on cloud computing that could impede privacy.

One proposal to help defuse some of the ethical dilemmas surrounding algorithmic decision-making calls for the establishment of "consumer privacy review boards," modeled after the human subject review boards (IRB) that operate in academic research institutions. Ryan Calo explains, "Today, any academic researcher who would conduct experiments involving people is obligated to comply with robust ethical principles and guidelines for the protection of human subjects."[100] He posits that by formalizing the review of new initiatives involving consumer data, policy managers could manage and head off regulatory risk, and more importantly, "add a measure of legitimacy to the study of consumers for profit."[101] A similar model could be implemented in states and school districts, to help vet ed tech projects and enhance the transparency and accountability of automated decisions affecting students and teachers.

---

[98] SIIA's Vision K20 finds that education's implementation of e-portfolios ranks last on a list of 20 ways that schools can more effectively use technology at just 1.35 on a scale of 1-4. *See Vision K-20 Survey Results*, SOFTWARE & INFO. INDUSTRY ASS'N, http://www.siia.net/visionk20/survey.asp (last visited Apr. 21, 2014).

[99] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH & INTELL. PROP. 239 (2013), *available at* http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip.

[100] Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 STAN. L. REV. ONLINE 97 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards.

[101] *Id.*

Technology: Equalizer or Divider?

Any assessment of technology and data use in the context of school reform is remiss without discussion of its impact on race and income inequalities. Unfortunately, in the United States today, broad disparities persist in the performance of African American and Hispanic students compared to their white counterparts. Similarly, students from higher income families resoundingly outperform those from lower income families. Much of the focus of education reform is targeted at identifying and measuring the gaps between these groups and testing the effectiveness of various efforts to narrow them. Such efforts are inextricably tied to detailed collection and tracking of sensitive student data.

Moreover, many ed tech and adaptive curricula initiatives are specifically tailored to assist lower performing students. Privacy advocates should be cautious of advocating reforms that might undermine the continued operation of such tools. In fact, solutions that rely heavily on legalistic parental notices or choice requirements may impede education reform in precisely those sectors that need it most. If individual students opt-out of the deployment of supplemental ed tech tools, or if their parents simply do not send in the required opt-in forms, those students may miss out. Meanwhile, private and charter schools, which are relatively free of regulatory obligations, will continue to bullishly implement ed tech and data solutions to advance student performance. In the marketing context, policymakers are not concerned if users do not opt-in to a service or are worried about privacy and opt-out. But in the education area, opting out may be akin to dropping-out.

It is also important to recognize that the school is no longer the entirety of a student's educational experience. Families are supplementing school with apps, tutoring centers, after-school clubs and informal learning. This includes high-poverty and minority students. As such, the robust information assembled about a student in school should be leveraged outside of school to create a more seamless and efficient learning process. Locking down the data in schools for fear that a vendor is inappropriately marketing will undermine the opportunities to empower families and others supporting students with the information and recommended learning modules that flow from that data. Just because the school is not providing that certain app or learning module should not mean the student loses the opportunity to discover its match to his or her unique learning needs.

Traditional privacy studies raise ire that the wealthy will benefit from privacy while the poor pay for free services with their data. In crafting privacy responses to ed tech disruption, policymakers must be careful to avoid causing the benefits of technology to accrue primarily to wealthier, more privileged and technology savvy audiences.

CONCLUSION

The influx of ed tech into classrooms and schools has provided education institutions with robust tools to improve teaching and instructional methods; diagnose students' strengths and weaknesses and adjust materials and approaches for individual learners; identify at-risk students so teachers and counselors can intervene early; and rationalize resource allocation and procurement decisions.

At the same time, it presents new risks to student privacy; raises big data concerns about unfairness and discrimination; and threatens to upend the delicate balance between stakeholders involved in education policy, including the federal and state governments, school districts, schools, teachers and parents as well as businesses, academic leaders and think tanks. It is critical that stakeholders move quickly to address any real gaps in school privacy, starting by ensuring that schools have the capacity for data governance, training of essential personnel, and basic auditing. Gaps in FERPA and COPPA must be filled to better adapt the legislation to current technological realities. More broadly, policymakers must ensure additional data transparency to engender trust, tapping into innovative solutions such as digital backpacks, data featurization and algorithm transparency. Without measures to help parents see clearly how data are used to help their children succeed, the debate about data in education will remain polarized. With them, ed tech will be further harnessed to democratize education, better tailor solutions for individual student needs, and provide objective metrics for measurement and improvement.