Who is Reading Whom Now: Privacy in Education from Books to MOOCs

Jules Polonetsky[*]
Omer Tene[**]

ABSTRACT

The arrival of new technologies in schools and classrooms around the nation has been met with a mixture of enthusiasm and anxiety. Education technologies ("ed tech") present tremendous opportunities: they allow schools to tailor programs to individual students; make education more collaborative and engaging through social media, gamification, and interactive content; and facilitate access to education for anyone with an Internet connection in remote parts of the world. At the same time, the combination of enhanced data collection with highly sensitive information about children and teens presents grave privacy risks. Indeed, in a recent report, the White House identified privacy in education as a flashpoint for big data policy concerns.

This Article is the most comprehensive study to date of the policy issues and privacy concerns arising from the surge of ed tech innovation. It surveys the burgeoning market of ed tech solutions, which range from free Android and iPhone apps to comprehensive learning management systems and digitized curricula delivered via the Internet. It discusses the deployment of big data analytics by education institutions to enhance student performance, evaluate teachers, improve education techniques, customize programs, and better leverage scarce resources to optimize education results.

This Article seeks to untangle ed tech privacy concerns from the broader policy debates surrounding standardization, the Common Core, longitudinal data systems, and the role of business in education. It unpacks the meaning of commercial data uses in schools, distinguishing between behavioral advertising to children and providing comprehensive, optimized education solutions to students,

* Jules Polonetsky is Co-chair and Executive Director of the Future of Privacy Forum.

** Omer Tene is a Senior Fellow at the Future of Privacy Forum.

The authors would like to thank Kelsey Finch and Joe Jerome for their excellent assistance with research and drafting.

teachers, and school systems. It addresses privacy problems related to "small data"—the individualization enabled by optimization solutions that "read students" even as they read their books—as well as concerns about "big data" analysis and measurement, including algorithmic biases, discreet discrimination, narrowcasting, and chilling effects.

This Article proposes solutions ranging from deployment of traditional privacy tools, such as contractual and organizational governance mechanisms, to greater data literacy by teachers and parental involvement. It advocates innovative technological solutions, including converting student data to a parent-accessible feature and enhancing algorithmic transparency to shed light on the inner working of the machine. For example, individually curated "data backpacks" would empower students and their parents by providing them with comprehensive portable profiles to facilitate personalized learning regardless of where they go. This Article builds on a methodology developed in the authors' previous work to balance big data rewards against privacy risks, while complying with several layers of federal and state regulation.

TABLE OF CONTENTS

"These days, however, New York politics seems to be all about education and it's hard to find any agreement on facts—let alone policy."

- John King, New York State Commissioner of Education and President of the University of the State of New York[1]

I. INTRODUCTION

A Positive View

Dave is a fourth grade student. In class, he watches as his teacher sketches out the solution to a math problem on her interactive smartboard. Back home, he can log into the classroom app on his tablet to review the teacher's notes as well as a short video showing her work through the problem. He then answers interactive questions and quizzes based on the lecture notes. His performance is automatically analyzed and he is steered to additional content, quizzes, and games that are tailored to his needs. He can communicate with his

1. John King, Comm'r, N.Y. State Educ. Dep't, Univ. of the State of N.Y., Address at New York University Policy Breakfast (Apr. 10, 2014), *available at* http://usny.nysed.gov/docs/nyu-policy-breakfast-2014.pdf.

classmates and teacher about these problems through a social learning platform, participate in polls, and contribute to his classroom blog. Through the platform, he submits his homework assignment and the teacher grades it and provides immediate personal feedback. The teacher can track and monitor the progress of Dave and his classmates through a dashboard, identifying children who need additional assistance as well as those who are ready for more challenging exercises. This helps her decide whether to reiterate an issue for the entire class or devote additional time to Dave, so that, although he does not display it in class, he can overcome his incomprehension. Dave's parents remain apprised of his progress through an app, which provides access to his every assignment, grade, and test score—even the slides and videos used in class. Dave's school obtains data helping it assess and adjust the fourth grade curriculum and evaluate the performance of students, classes, and teachers. The local school district judges the performance of Dave's school and reports aggregate, anonymous data to the state department of education. Funding is directed to schools that are successful at improving children's readiness for college and to districts that hold teachers accountable for student performance.

A Negative View

Dave is a fourth grade student. His interaction with his teacher has become entirely mediated by screens, including tablets, software, dashboards and apps. Algorithms that crunch through his every keystroke and page-view constantly assess him. His school experience focuses on test preparation, evaluations, and exams. The software used by his school is made by a for-profit company, and vendors, which are advised by think-tank experts, develop the curriculum and tests. The school has put Dave's teacher on probation since she "couldn't make her target numbers." Her plea to reason, arguing that her students have special needs and should not be judged against national or state metrics, fails to impress her principal, who is also under increasing pressure from the school district and state to improve student performance, as judged by standardized test scores. The data collected from Dave and his classmates is stored by a cloud service provider, which centrally hosts sensitive information from hundreds of schools. Fifteen years later, as Dave seeks to enter the workforce, a prospective employer inquires about his suspension from Ms. Smith's fourth grade class.

Education is changing—online curricula and tools proliferate; use of social media and cloud applications for file storage, and note

taking and collaboration have 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 to knowledge 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. Furthermore, data is increasingly being used to hold schools and educators accountable for student performance.

On the one hand, these new education technologies ("ed tech") bring tremendous promise to the world of education. 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 world. They have democratized and spread education across national, socioeconomic, and age boundaries, with education app usage booming in emerging economies such as India, South Africa, Kenya, and Nigeria.[2] They allow students to broaden their horizons through openly available lectures from the best professors at world-renowned universities such as Stanford, Harvard and MIT, while also benefitting from automated, individualized tutoring and adaptive learning tools that help strong students surge forward and weaker students keep pace.

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 ed tech efforts misguided, labeling them as the work of "corporate education reformers" who seek 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.[3] These advocates call instead for entirely different education solutions that—while perhaps not excluding technological innovations—are focused on smaller classes and higher

2. *See Growth Markets Demonstrate the Value of Mobile Education Apps*, THEMARKETINGSITE.COM, http://www.themarketingsite.com/knowledge/37038/growth-markets-demonstrate-the-value-of-mobile-education-apps (last visited Apr. 17, 2015).

3. CATHY N. DAVIDSON & DAVID THEO GOLDBERG, THE FUTURE OF LEARNING INSTITUTIONS IN A DIGITAL AGE (2009), *available at* https://mitpress.mit.edu/sites/default/files/titles/free_download/9780262513593_Future_of_Learning.pdf; DIANE RAVITCH, REIGN OF ERROR: THE HOAX OF THE PRIVATIZATION MOVEMENT AND THE DANGER TO AMERICA'S PUBLIC SCHOOLS (2013).

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 rather than learning, and school systems obsess over numbers instead of student welfare.

Policymakers at the highest levels of government have recognized the tension between ed tech opportunities and concerns about privacy and civil liberties. In its recent report, *Big Data: Seizing Opportunities, Preserving Values* (the "White House Report"), the White House recommended that Congress:

> [M]odernize the privacy regulatory framework under the Family Educational Rights and Privacy Act and Children's Online Privacy Protection Act 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.[4]

The debate is fraught with emotions. Teachers fear for their jobs, and parents are anxious about their children's future. And schools are 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 ecosystem while avoiding data breaches and privacy snafus. Even without the political overtones, the issues are complex and highly nuanced. How persistent should student data be? Should a school suspension in fourth grade come back to haunt a student as he enters the workforce?[5] Are *any* commercial uses of student data legitimate? For example, should a vendor be allowed to analyze the performance of a student on a math app in order to recommend to her an advanced level upgrade? 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.

This Article, which focuses particularly on K–12 education concerns but also addresses broader issues affecting higher education, seeks to disentangle the privacy problems at stake from the separate education policy debates raging around technology and standardization. It posits that privacy concerns—such as ensuring

---

4. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 64 (May 2014) [hereinafter WHITE HOUSE REPORT], *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

5. Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, N.Y. TIMES, Nov. 9, 2013, http://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html.

that proper data governance mechanisms exist for both educational institutions and private sector vendors, delineating legitimate uses of children's information, and determining retention periods and access rights—can and should be resolved through modest reforms of the current system. More novel ethical problems arising from the deployment of big data technologies in schools should be addressed with a toolkit comprising innovative solutions, including data "featurization" and enhanced algorithmic transparency.

Part II of this Article lays out the brave new world of ed tech, including a discussion of the innovative tools and services for administering schools, delivering curricula, measuring performance, and optimizing results. It highlights key trends such as the migration of student data to the cloud, the introduction into classrooms of student- and school-owned devices and a wide variety of apps, the development of digital content and instructional software as well as social media platforms dedicated to education, and the emergence of the massive online open courses (MOOCs) at veritable online institutions for higher education. It describes the development of optimization platforms, which adapt to students' behavior and reactions as they interact with digital content, essentially "reading" the students as they read their books.

Part III tracks the policy concerns resulting from ed tech innovation that transcend the privacy debate. These include highly politicized controversies around the role of the federal government in education, standardization of curricula and tests through the Common Core, and the allocation of responsibilities between school administrators, teachers, and parents. To help extinguish what has been a fiery debate, it seeks to separate policy issues about the future of education from more technical privacy concerns.

Part IV directly addresses the traditional privacy concerns surrounding school and vendor management, including contracting and data security. To do so, it unpacks the various meanings of commercialization in schools, some of which are data driven while others are not. It proceeds with an in-depth review and critique of the current regulatory regime affecting the commercialization of student data. Finally, it sets forth a path for resolving traditional privacy issues, questioning the validity of imposing the brunt of data governance mainly on vendors as opposed to governments and schools. It calls for the institution of data governance mechanisms in the education system, including privacy training, appointment of privacy officers, model communications with parents, and de-identification tools.

Part V turns to the ethical concerns implicated by the brave new world of big data capabilities in schools. It addresses concerns

over unfairness and discrimination, narrowcasting and filter bubbles, predictive sorting, and the stratification of society into "haves" and "have nots." To mitigate these issues, it calls for empowerment of parents through data "featurization" and enhanced algorithmic transparency. At the same time, it cautions against solutions that could impoverish already weak populations, accentuating, instead of helping to solve, a broadening technological divide.

II. ED TECH INNOVATION

Ed tech is revolutionizing classrooms, schools, and school systems, affecting the relationship between students and educators, the internal and statewide management of schools, and school performance assessments and accountability vis-à-vis parents and budgetary sources. This Part provides a comprehensive overview of ed tech innovations, which are divided into four categories: *administrative technologies*, which draw on cutting-edge information technologies to help more effectively, efficiently, and securely manage schools; *delivery systems*, which help augment—and, some fear, replace—traditional learning tools such as books and whiteboards with a dizzying array of hardware, software, and cloud-based content, social tools, and data management solutions; *measurement tools*, which deploy state-of-the-art big data analytics to parse student and school information for important lessons and findings; and *optimization programs*, which enable personalized and adaptive learning by continually customizing material based on student input.

A. Administrative Technologies

Information technology developments in the field of education closely track those in other industry sectors. Traditional administrative school functions, which were once managed offline and documented on papers that were maintained in file cabinets, are now computerized and increasingly stored in the cloud.[6] Enterprise resource planning (ERP) systems streamline districts' entire operation centers into cloud-based warehouses, managing everything from student records to accounting, equipment, and facilities information

6. *See* Kenneth C. Green, *The 2013 Campus Computing Survey*, CAMPUS COMPUTING PROJECT (Oct. 17, 2013), http://www.campuscomputing.net/sites/www.campuscomputing.net/files/CampusComputing2013_1.pdf; MICROSOFT, BIG DATA: THE NEW DIGITAL CAMPUS, *available at* http://www.microsoft.com/education/ww/solutions/Documents/digital-campus_Bigdata_F.docx (last visited Apr. 17, 2015).

technology (IT).[7] Cloud services have become ubiquitous; according to a recent study, 95 percent of public school districts rely on them.[8] New technologies, such as biometrics, are also harnessed to manage day-to-day school activities, including cashless cafeterias, library loans, and locker systems.[9] With online and distance learning programs proliferating around the world, educational institutions are deploying facial recognition, keystroke screening, and other technologies to deter remote users from gaming their systems and ensure the integrity of learning and assessment tools.[10]

B. Delivery Systems

Technology now mediates practically every educational school activity. This includes class scheduling, lectures, remote learning, testing, grading, email services, teacher websites, blogs, social networks, and more. Moreover, the use of technology for the delivery of learning and education should not come as a surprise. It reflects a

---

7. *See* GREG KEARSLEY & WILLIAM LYNCH, EDUCATIONAL TECHNOLOGY: LEADERSHIP PERSPECTIVES 40 (1994); BARBARA MEANS ET AL., U.S. DEP'T OF EDUC., USE OF EDUCATION DATA AT THE LOCAL LEVEL: FROM ACCOUNTABILITY TO INSTRUCTIONAL IMPROVEMENT (2010), *available at* http://www2.ed.gov/rschstat/eval/tech/use-of-education-data/use-of-education-data.pdf; MICROSOFT, *supra* note 6; Dave Swartz & Ken Orgill, *Higher Learning ERP: Lessons Learned*, 2 EDUCAUSE Q. 20 (2001), *available at* https://net.educause.edu/ir/library/pdf/eqm0121.pdf.

8. JOEL REIDENBERG ET AL., FORDHAM CTR. L. & INFO. POL'Y, PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS (Dec. 2013) [hereinafter CLIP STUDY], *available at* http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip.

9. *See* Anita Ramasastry, *Biometrics in the School Lunch Line: Why Parents Should Be Concerned About the Privacy Implications of This Trend*, VERDICT (Oct. 9, 2012), http://verdict.justia.com/2012/10/09/biometrics-in-the-school-lunch-line; Wylie Wong, *Biometrics Goes to School*, EDTECH (Oct. 31, 2006), http://www.edtechmagazine.com/k12/article/2006/10/biometrics-goes-to-school.

10. *See Coursera Offers Biometric-based 'Verified Certificates' for a Fee, Extends Credential Options for Students*, ICEF MONITOR (Jan. 10, 2013), http://monitor.icef.com/2013/01/coursera-offers-biometric-based-verified-certificates-for-a-fee-extends-credential-options-for-students/; Patricia A. Aceves & Robert I. Aceves, *Student Identity and Authentication in Distance Education: A Primer for Distance Learning Administrators*, 73 CONTINUING HIGHER EDUC. REV. 143 (2009), *available at* http://files.eric.ed.gov/fulltext/EJ903458.pdf. Software and Information Industry Association (SIIA), which represents many education technology companies, explains that retina and fingerprint biometrics are used for identification and security in the context of online testing and virtual learning, as well as for helping secure student data on devices. *See, e.g.*, Letter from Mark Schneiderman on behalf of Software & Info. Industry Ass'n, to Educ. Comm., Ga. H.R., RE: LC 34 4241ERS substitute to SB 167, Part II (Mar. 11, 2014). Use of biometric data for instructional purposes includes voice to text for hearing impaired students, voice recording and diagnostics for reading or foreign language learning, and eye tracking for diagnostics in reading comprehension. In many cases, this data need not be identifiable or retained, thus reducing privacy concerns. Where it is necessary for the biometric data to be collected or personally identifiable, alternative protections include restrictions on inclusion in a student's permanent educational record, requirements for deletion, and other security measures such as encryption to protect unauthorized access.

general societal trend toward technology-mediated content distribution and consumption. As the US Department of Education recently noted:

> Gone are the days when textbooks, photocopies, and filmstrips supplied the entirety of educational content to a classroom full of students. Today's classrooms increasingly employ on-demand delivery of personalized content, virtual forums for interacting with other students and teachers, and a wealth of other interactive technologies that help foster and enhance the learning process. Online forums help teachers share lesson plans; social media help students collaborate across classrooms; and web-based applications assist teachers in customizing the learning experience for each student to achieve greater learning outcomes.[11]

Technological developments in the delivery space include learning management systems (LMS), which provide an accessible, interactive infrastructure for sharing course content.[12] Devices, such as laptops and tablets, have changed the learning environment in classrooms.[13] Education apps have become a surging industry sector in their own right,[14] as have social media platforms, including general audience sites that are repurposed for classroom interactions, as well as dedicated services that create an educational community comprising teachers, parents, and students.[15] Game-based learning

---

11. PRIVACY TECHNICAL ASSISTANCE CTR., U.S. DEP'T OF EDUC., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 1 (Feb. 2014) (hereinafter DOE ONLINE GUIDANCE), *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf.

12. *See* Xin Song, *Recent Trends & the Future of Educational Technology*, DATA FOX (Apr. 4, 2014), http://www.datafox.co/blog/educational-technology-industry-analysis-key-players-future-trends/; William R. Watson & Sunnie Lee Watson, *An Argument for Clarity: What Are Learning Management Systems, What Are They Not, and What Should They Become?*, 51 TECH. TRENDS 28 (2007), *available at* http://link.springer.com/article/10.1007/s11528-007-0023-y#page-2.

13. *See* Chris Riedel, *10 Major Technology Trends in Education*, THE JOURNAL (Feb. 3, 2014), http://thejournal.com/Articles/2014/02/03/10-Major-Technology-Trends-in-Education.aspx?Page=1 ("The 2013 results represent more than 400,000 surveys from 9,000 schools and 2,700 districts across the country."); *Vision K–20 Survey Results*, SOFTWARE & INFO. INDUSTRY ASS'N, http://www.siia.net/visionk20/survey.asp (last visited Apr. 21, 2014).

14. *See* APPLE, APPS IN THE CLASSROOM (2013), *available at* https://ssl.apple.com/education/docs/L523172A_EDU_App_Guide_062013.pdf; CARLY SHULER ET AL., THE JOAN GANZ COONEY CENTER, iLEARN II; AN ANALYSIS OF THE EDUCATION CATEGORY OF THE iTUNES APP STORE (Jan. 2012), *available at* http://www.joanganzcooneycenter.org/wp-content/uploads/2012/01/ilearnii.pdf; Preeti Upadhyaya, *How Apple, Google, Cisco Are Competing for the $5 Billion K-12 Ed-Tech Market*, SILICON VALLEY BUS. J. (Nov. 25, 2013, 11:01 AM), http://www.bizjournals.com/sanjose/news/2013/11/25/heres-how-silicon-valley-will-make.html?page=all.

15. *See* L. JOHNSON ET AL., NEW MEDIA CONSORTIUM, NMC HORIZON REPORT: 2014 HIGHER EDUCATION EDITION (2014), *available at* http://www.nmc.org/pdf/2014-nmc-horizon-report-he-EN.pdf; Vicki Davis, *A Guidebook for Social Media in the Classroom*, EDUTOPIA (Feb. 27, 2014), http://www.edutopia.org/blog/guidebook-social-media-in-classroom-vicki-davis; Lori Grisham, *Teachers, Students and Social Media: Where Is the Line?*, USA TODAY (Apr. 9, 2014,

and gamification tools increase student engagement by stimulating fun and creativity.[16] Digital badges and ePortfolios provide an online environment for student assessment and credentialing.[17] Digital content and instructional software proliferate[18] and the market is fast opening to the arrival of MOOCs,[19] where technology vendors not only create the curriculum but become educational institutions in their own right.

As one-to-one computing in classrooms and students' use of social media grows, educational and general platforms are beginning to consolidate services aimed at teachers with those targeted at students. For example, Google's "Apps for Education" suite will soon be adding a "Classroom" service to help teachers create, distribute, collect, and grade assignments online, while also providing a platform for teachers and students to communicate in real time.[20] These chimeric, all-in-one offerings bring together traditional LMS tools and emerging social teaching trends in order to ease the clerical and administrative burden that dispersed technologies impose on teachers, giving "teachers more time to teach and students more time to learn."[21]

6:54 PM), http://www.usatoday.com/story/news/nation-now/2014/04/09/facebook-teachers-twitter-students-schools/7472051/.

16. *See Gamification Infographic*, KNEWTON, http://www.knewton.com/gamification-education/ (last visited Apr. 17, 2015); *What is GBL (Game-Based Learning)?*, EDTECHREVIEW (Apr. 23, 2014), http://edtechreview.in/dictionary/298-what-is-game-based-learning; David Raths, *The 10 Biggest Trends in Ed Tech*, THE JOURNAL (Jan. 6, 2014), http://thejournal.com/articles/2013/12/13/the-10-biggest-trends-in-ed-tech.aspx.

17. *See* GEORGE LORENZO & JOHN ITTELSON, EDUCAUSE LEARNING INITIATIVE, AN OVERVIEW OF E-PORTFOLIOS (2005), *available at* https://net.educause.edu/ir/library/pdf/eli3001.pdf; *Digital Badges*, MACARTHUR FOUND., http://www.macfound.org/programs/digital-badges/ (last visited Apr. 22, 2014).

18. *See* Tommy Peterson, *How Districts Are Preparing for Common Core and Other Online Testing Initiatives*, EDTECH (Jan. 7, 2013), http://www.edtechmagazine.com/k12/article/2013/01/how-districts-are-preparing-common-core-and-other-online-testing-initiatives; JOHN RICHARDS ET AL., SOFTWARE & INFO. INDUSTRY ASS'N, 2013 U.S. EDUCATION TECHNOLOGY MARKET: PREK–12, (2013); Donald Watkins, *The Rise of Digital Textbooks and OER*, CK–12 (Oct. 21, 2013), http://www.ck12.org/blog/the-rise-of-digital-textbooks-and-oer/.

19. *See* James Grimmelmann, *The Merchants of MOOCs*, 44 SETON HALL L. REV. 1035 (2014); Clay Shirkey, *Napster, Udacity, and the Academy,* SHIRKEY (Nov. 12, 2012), http://www.shirky.com/weblog/2012/11/napster-udacity-and-the-academy/; Kate Torgovnick May, *Completely Free Online Classes? Coursera.org Now Offering Courses from 16 Top Colleges*, TED BLOG (July 18, 2012, 9:48 AM), http://blog.ted.com/2012/07/18/completely-free-online-classes-coursera-org-now-offering-courses-from-14-top-colleges/comment-page-3/ (quoting Coursera co-founder Daphne Koller).

20. *See Previewing A New Classroom*, GOOGLE BLOG (May 6, 2014), http://googleblog.blogspot.com/2014/05/previewing-new-classroom.html.

21. *Id.*

C. Measurement Tools

Ed tech is used not only to deliver education but also to measure the performance of students, teachers, and schools.[22] Data analysis techniques facilitate immediate real-time feedback loops, which help decision makers efficiently allocate resources, gauge the effectiveness of curricular programs, manage schools and classrooms, and tailor education to the needs of individual students.[23] This student data comprises not only information on transcripts—such as personal details, test scores, individual assignments, and course grades—but also a host of other personally identifiable information[24] that is used for a wide range of purposes within the education system.[25] For example, longitudinal data systems are used to analyze school, teacher, and student performance across time and geographies.[26]

But collecting student data is not a recent phenomenon. In fact, schools have always been collectors of massive troves of information about students.[27] Traditionally, schools kept student data in paper files or disparate software silos. But increasingly, forces of both demand and supply have pushed for aggregation of student data and integration with analytics tools.[28] The combination can provide schools with insights into multiple aspects of students' lives and aid governments by offering an accurate assessment of school and teacher

---

22. George Siemens & Phil Long, *Penetrating the Fog: Analytics in Learning and Education*, 46 EDUC. REV. 30 (2011).

23. *See* INST. EDUC. SCIS., NAT'L CTR. FOR EDUC. STATISTICS, SLDS TECHNICAL BRIEF: GUIDANCE FOR STATEWIDE LONGITUDINAL DATA SYSTEMS (SLDS) (Nov. 2010) (hereinafter SLDS TECHNICAL BRIEF), *available at* http://nces.ed.gov/pubs2011/2011602.pdf.

24. *Id.* Such as demographics, financial information, attendance, behavioral and disciplinary records, health records, food preferences and allergies, vaccinations, library check-outs, sports participation, cafeteria and bookstore purchases, times in and out of a dormitory, and use of a school's online services including email and web browsing. *See id.*

25. *See id.* For example, handling inquiries from prospective students, managing application and admissions processes, automatically generating class and teacher schedules, handling records of tests and assessments, grades and academic progression, maintaining records of absences and attendance, keeping disciplinary records, producing statistical reports, managing transportation and cafeteria services, storing health records and collecting tuition fees. *See id.*

26. *See* discussion *infra* Part III.B (addressing the role of business in education).

27. *See* Bill Fitzgerald, *Data Collection Isn't New. And It Predates Common Core.*, FUNNYMONKEY (Jan. 6, 2014), http://funnymonkey.com/blog/data-collection-isnt-new-and-it-predates-common-core.

28. *See* Benjamin Herold, *inBloom to Shut Down Amid Growing Data-Privacy Concerns*, EDUC. WK. (Apr. 21, 2014, 10:33 AM), http://blogs.edweek.org/edweek/DigitalEducation/2014/04/inbloom_to_shut_down_amid_growing_data_privacy_concerns.html?cmp=SOC-SHR-TW.

performance.[29] With time, this data could also incorporate granular information gleaned from adaptive learning tools, helping schools follow individual student activity down to the last keystroke.[30]

D. Optimization Programs

The introduction of education software and apps into classrooms has enabled a previously unimaginable degree of personalization.[31] In fact, it is conceivable that every student will soon have their teacher supplemented with a personal tutor, carefully calibrating content, assignments, and tests to his personal skills. Moreover, that tutor will be written in binary code.[32] Education software not only tailors programs to students' individual pace of learning, skills, and preferences, but also allows schools to accurately and continuously gauge student performance.[33] The development of computerized learning modules enables teachers and schools to assess students in systematic yet personalized ways.[34] At the same time, the deployment of devices in classrooms and students' engagement with free apps implicates a data play that raises concerns in the context of children's data.[35]

After only a few generations of evolution, optimization tools now provide real-time assessments so that class material can be presented to students based on an individual assessment of how fast and effectively they learn.[36] Education technologies can also be scaled to reach broad audiences, enable continuous improvement of course

---

29. *U.S. Education Department Announces New Measures to Safeguard Student Privacy*, U.S. DEPT. EDUC. (Dec. 1, 2011), http://www.ed.gov/news/press-releases/us-education-department-announces-new-measures-safeguard-student-privacy.

30. *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/ (transcribing as well as providing notes and slides for Ms. Watters's October 16, 2013 talk at Columbia University).

31. OFFICE OF EDUC. TECH., U.S. DEPT. EDUC., ENHANCING TEACHING AND LEARNING THROUGH EDUCATIONAL DATA MINING AND LEARNING ANALYTICS (2012), *available at* http://www.cra.org/ccc/files/docs/learning-analytics-ed.pdf.

32. TYTON PARTNERS, LEARNING TO ADAPT: UNDERSTANDING THE ADAPTIVE LEARNING SUPPLIER LANDSCAPE (2013), *available at* http://tytonpartners.com/tyton-wp/wp-content/uploads/2015/01/Learning-to-Adapt_Supplier-Landscape.pdf.

33. John K. Waters, *The Great Adaptive Learning Experiment*, CAMPUS TECH. (Apr. 16, 2014), http://campustechnology.com/Articles/2014/04/16/The-Great-Adaptive-Learning-Experiment.aspx?Page=1.

34. John K. Waters, *Adaptive Learning: Are We There Yet?*, THE JOURNAL (May 14, 2014), http://thejournal.com/Articles/2014/05/14/Adaptive-Learning-Are-We-There-Yet.aspx.

35. *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/.

36. DOE ONLINE GUIDANCE, *supra* note 11.

content, and increase student engagement.[37] As the White House recently noted, "Beyond personalizing education, the availability of new types of data profoundly improves researchers' ability to learn about learning."[38] At the same time, the abundant collection of student data, its storage and use to measure and optimize performance, and the role of for-profit businesses in education raise challenging policy dilemmas that must be dealt with to mitigate risks to privacy and civil liberties and cultivate trust from relevant stakeholders.

III. UPENDING THE EXISTING BALANCE

Collecting and using students' data has always been key for the effective administration of school systems. One commentator characterized schools as "information-collection machines" that aggregate 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.[39] Schools have long collected and maintained essential, sensitive information about children—data needed to administer their core academic activities and societal mission. But in reality, education has long been data rich and information poor. That is, the education system collected data but in formats and into silos that made it inaccessible and unactionable.

The recent introduction of big data technologies into the field of education has threatened to upset the delicate balance between national and local policymaking, and education experts and local teacher unions. Education reformers view the industrial-age educational model as outdated, inefficient, and ineffective. They warn that self-interested, entrenched stakeholders will unnecessarily impede educational innovation. Critics, in turn, perceive technology vendors as advancing an agenda created in Silicon Valley and Washington, DC that is driven by powerful business interests and touted by academic think tanks.[40]

---

37. Anya Kamenetz, *What If You Could Learn Everything?*, NEWSWEEK (July 10, 2013, 4:45 AM), http://www.newsweek.com/2013/07/10/what-if-you-could-learn-everything-237660.html.

38. WHITE HOUSE REPORT, *supra* note 4, at 24.

39. Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public Schoolchildren*, 84 NEB. L. REV. 1158, 1159 (2006).

40. Some commentators claimed that the personal involvement of public figures such as Rupert Murdoch, Bill Gates, and the former Chancellor of the New York City Department of Education Joel Klein in inBloom stoked the fire of public criticism that eventually consumed the ed tech innovator. Bill Fitzgerald, *Student Privacy, Data Collection, inBloom, and Having an Informed Conversation*, FUNNYMONKEY (Nov. 19, 2013), http://funnymonkey.com/blog/student-

As a result of these new technologies, students and teachers alike find themselves under an algorithmic magnifying glass. The federal government continues to push hard for evaluation of teacher education programs by several key metrics, such as how many graduates land teaching jobs, how long they stay in the profession, and whether they boost their students' scores on standardized tests and other student performance measures. For example, the Obama Administration intends to steer financial aid, including nearly $100 million a year in federal grants, to those teacher prep programs that score the highest on standardized measurement metrics. According to the Secretary of Education, Arne Duncan, the rest will need to improve or "go out of business."[41]

A. Datafication

The 1983 Reagan administration report "A Nation at Risk" invigorated the "datafication" of American schools, warning that students in the United States were falling behind those in other countries. It called for a new focus on "content" and more rigorous and measurable standards.[42] The movement gained momentum with the No Child Left Behind Act (NCLBA), signed into law by President George W. Bush in 2001.[43] By requiring schools to measure and report student performance disaggregated by various characteristics, NCLBA boosted the adoption of ed tech in state-funded schools. Continuing this trend, President Barack Obama's 2009 Race to the Top initiative dedicated more than $4 billion to nineteen states that embraced an agenda of education innovation in K–12 schools, including development of rigorous standards and better assessments; adoption of better data systems to provide schools, teachers, and parents with information about student progress; and increased emphasis and resources for turning around the lowest-performing schools.

Virtually all states participating in the Race to the Top initiative developed robust longitudinal data systems. To secure federal funding, state data systems must be able to follow students

---

privacy-data-collection-inbloom-and-having-informed-conversation; Andrea Gabor, *inBloom, Education Technology and the Murdoch-Klein Connection: A Son-of-Frankenstein B-movie Sequel?*, ANDREA GABOR (Oct. 8, 2013), http://andreagabor.com/2013/10/08/inbloom-education-technology-and-the-murdoch-klein-connection-a-son-of-frankenstein-b-movie-sequel.

41. *See* Stephanie Simon, *Barack Obama Cracks Down on Poor Teacher Training*, POLITICO (Apr. 25, 2014, 6:02 AM), http://www.politico.com/story/2014/04/barack-obama-arne-duncan-teacher-training-education-106013.html.

42. NAT'L COMM'N ON EXCELLENCE IN EDUC., A NATION AT RISK: THE IMPERATIVE FOR EDUCATIONAL REFORM, A REPORT TO THE NATION AND THE SECRETARY OF EDUCATION (Apr. 1983), *available at* http://datacenter.spps.org/uploads/SOTW_A_Nation_at_Risk_1983.pdf.

43. No Child Left Behind Act, Pub. L. No. 107-110, 115 Stat. 1425 (2002).

from pre-kindergarten through college, logging information about students' grades, including details about when they graduate or drop out. States are also expected to match teachers with their students' performance over time.[44] In addition, states developed or procured data "dashboards" or "portals" for educators to analyze student performance data and other school-related data. "[A]gency staff provided training for educators to help them use statewide data systems, especially for instructional improvement."[45]

The Race to the Top initiative further incentivized states to adopt the Common Core standards. Initially conceived as a state-led effort driven by the National Governors Association and the Council of Chief State School Officers (CCSSO), the Common Core sought to establish consensus on the expectations for student knowledge and skills in grades K–12.[46] Released in 2010, it represented an unprecedented shift away from disparate content guidelines across individual states in the areas of English language, arts, and mathematics. By 2014, forty-three states and the District of Columbia had adopted the Common Core.[47]

The deployment of Common Core has generated heated controversy and met stiff resistance from an odd coalition of state lawmakers, conservative groups, tea party members, teacher unions, parents and school boards.[48] Some conservatives are depicting the adoption of Common Core, dubbed "Obamacore," as a backdoor through which the federal government sought to usurp local control of education in order to implement a national curriculum.[49] Teacher unions are concerned that new tests aligned to the standards will be used not only to evaluate students but also to evaluate and discipline

---

44. *See* Tiffany D. Miller & Robert Hanna, *Four Years Later, Are Race to the Top States on Track?,* CTR. FOR AM. PROGRESS (Mar. 24, 2014), http://www.americanprogress.org/issues/education/report/2014/03/24/86197/four-years-later-are-race-to-the-top-states-on-track/.

45. *See id.*

46. COUNCIL OF CHIEF STATE SCH. OFFICERS & NAT'L GOVERNORS ASS'N CTR. FOR BEST PRACTICES, COMMON CORE STATE STANDARDS INITIATIVE: PREPARING AMERICA'S STUDENTS FOR COLLEGE & CAREER (2010); *Development Process*, COMMON CORE STATE STANDARDS INITIATIVE, http://www.corestandards.org/about-the-standards/development-process/#timeline-2010 (last visited Apr. 17, 2015).

47. *Standards in Your State*, COMMON CORE STATE STANDARDS INITIATIVE, http://www.corestandards.org/standards-in-your-state/ (last visited Apr. 17, 2015).

48. *See* Jonathan Martin, *Republicans See Political Wedge in Common Core*, N.Y. TIMES (Apr. 19, 2014), http://www.nytimes.com/2014/04/20/us/politics/republicans-see-political-wedge-in-common-core.html.

49. See Kathleen Porter-Magee & Sol Stern, *The Truth about Common Core*, NATIONAL REV. (Apr. 3, 2013, 4:00 AM), http://www.nationalreview.com/articles/344519/truth-about-common-core-kathleen-porter-magee%20.

teachers.[50] Certain education experts have said the Common Core represents a "utilitarian view of education" that is overly focused on testing, data, and accountability.[51] They have decried the Common Core as driving a culture of test preparation as opposed to learning and called for a more nuanced approach to gauge the progress of K–12 students.[52]

The debate continues to build. The federal government, under both Democratic and Republican presidents, is leveraging its budget resources to advance efforts to accurately assess teacher and school performance under No Child Left Behind and Race to the Top, even as some states are passing legislation to restrict such efforts.

With this in mind, it is important to separate the Common Core discussion from the implications of datafication in schools. Regardless of prevailing education policy choices concerning curricula, assessment, and testing, schools are becoming increasingly reliant on data technologies, and those raise inevitable policy concerns. The drive toward implementation of statewide longitudinal data systems predates and transcends the development of Common Core.[53] State adoption of longitudinal data systems reflects a realization that in order to ensure accountable education systems, records must be maintained and linked across K–12 education and into the workforce. States started implementing longitudinal data systems in the 1980s, thirty years before Common Core, with the blessing and support of the federal government. To be sure, funding from the federal government has also been used to encourage the adoption of Common Core; yet onboarding the standards did not necessarily entail any new data collection requirements.[54] Rather, school districts across the country embraced longitudinal data systems in order to facilitate research and analysis, increase student achievement, and close achievement gaps.[55]

---

50. *See* Valerie Strauss, *NY Teachers Union Pulls Its Support from Common Core, Urges Removal of State Ed Chief*, WASH. POST (Jan. 26, 2014), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/01/26/ny-teachers-union-pulls-its-support-from-common-core-urges-removal-of-state-ed-chief.

51. Charles Upton Sahm, *The Incredibly Stupid War on the Common Core*, DAILY BEAST (Apr. 21, 2014, 5:45 AM), http://www.thedailybeast.com/articles/2014/04/21/the-incredibly-stupid-war-on-the-common-core.html.

52. *See* Diane Ravitch, *Why Doesn't the New York Times Understand the Controversy Over Common Core?*, DIANE RAVITCH'S BLOG (Apr. 20, 2014), http://dianeravitch.net/2014/04/20/why-doesnt-the-new-york-times-understand-the-controversy-over-common-core/.

53. Fitzgerald, *supra* note 27.

54. *See Frequently Asked Questions*, COMMON CORE STATE STANDARDS INITIATIVE, http://www.corestandards.org/about-the-standards/frequently-asked-questions (last visited Apr. 17, 2015).

55. *See* SLDS TECHNICAL BRIEF, *supra* note 23.

B. The Role of Business in Education

Questions surrounding the role of business in education transcend the discussion of privacy and require sensitive public policy choices by educators, social scientists, and economists. The idea that technology can revolutionize education is not new. For more than a century, almost every new invention—from typewriters and televisions to computers and the Internet—was heralded as shepherding a new technological era in schools. Yet, in the near past, innovative technologies merely provided schools and teachers with new tools to fulfill their mission. Today's debate is increasingly focused on whether technology has begun to usurp, or at least transform, roles traditionally occupied by teachers and schools.

Tech enthusiasts argue that technology and data empower teachers to improve their skills—ed tech provides critical feedback about what is or is not working for individual students and different classes of students and helps differentiate instruction through online repositories of otherwise unavailable teaching and learning resources. Conversely, critics lament what they view as an overinvestment in technology and data, arguing it reflects a long-term pattern of treating teachers like factory workers who are trained to be efficient, measured, assessed and ultimately terminated based on performance statistics.[56] Counter-reformers maintain that economic disparity is the overwhelming factor determining student performance, making it unfair to overemphasize teacher performance statistics. And the debate cycle continues, with reformers arguing that the current system of education treats students like widgets and needs to adapt to the unique needs of each student, and that it significantly underinvests in technology relative to nearly all other sectors of the economy.

According to a report by the American Statistical Association (ASA), however, formulas for measuring how much "value" a teacher adds to a student's test scores are complex and often have a sizable margin of error.[57] The ASA suggested that such formulas must be used with caution because teachers generally account for less than 14 percent—and in some studies as little as 1 percent—of the variability in student test scores, with the majority of opportunities for quality improvement found in system-level conditions. The ASA concluded that, although value-added models spin out precise-sounding numbers that purport to quantify a teacher's impact on

56. *See, e.g.*, RAVITCH, *supra* note 3.

57. *ASA Statement on Value-Added Models for Educational Assessment*, AM. STATISTICAL. ASS'N (Apr. 8, 2014), http://www.amstat.org/policy/pdfs/ASA_VAM_Statement.pdf.

students, the formulas in fact "measure correlation, not causation," thus conflating cause and effect and throwing policymaking efforts off track.[58] Another recent study, commissioned by the Department of Education, found that value-added measures fluctuate significantly due to idiosyncratic factors beyond teachers' control, including events as random as a dog barking loudly outside a classroom window that cause class scores to fluctuate.[59]

Critics of teacher measurement also point to the success of school systems in other countries that pay teachers well, hire teachers who are subject-matter experts, and keep class sizes small.[60] They point out that datafication has had the opposite effect, leading to large classes mediated by technology and "assembly line" teachers who are too focused on measurements rather than concentrating on mentoring individual students.[61] They lament the decline of the status of the American teacher from a respected leader with deep subject-matter expertise to an education industrial worker who is evaluated by student throughput and fired for missing a target.[62] They point to Rita Kramer's 1991 book, *Ed School Follies: The Miseducation of America's Teachers*,[63] which blasted schools of education for giving the nation "a steady stream of intellectually mediocre teachers who had been steeped in dubious educational theories, but often knew little about the subject matter they were to teach."[64]

Furthermore, critics argue that local teachers, not national companies and think tanks, should set the education agenda and curriculum for schools. They think that by missing the nuance and complexity of human interactions, automated systems unfairly

---

58. *See* Simon, *supra* note 41.

59. DAVID STUIT ET AL., U.S. DEP'T EDUC., COMPARING ESTIMATES OF TEACHER VALUE-ADDED BASED ON CRITERION- AND NORM-REFERENCED TESTS (Jan. 2014), *available at* http://ies.ed.gov/ncee/edlabs/regions/midwest/pdf/REL_2014004.pdf.

60. *See* Leonie Haimson, *Why Class Size Matters*, Parents Across Am., http://parentsacrossamerica.org/what-we-believe-2/why-class-size-matters/ (last visited Apr. 17, 2015).

61. *See* MCKINSEY & CO., HOW THE WORLD'S BEST PERFORMING SCHOOLS COME OUT ON TOP (Sept. 2007), *available at* http://www.smhc-cpre.org/wp-content/uploads/2008/07/how-the-worlds-best-performing-school-systems-come-out-on-top-sept-072.pdf; DIANE WHITMORE SCHANZENBACH, NAT'L EDUC. POLICY CTR., DOES CLASS SIZE MATTER?, (Feb. 2014), http://www.classsizematters.org/wp-content/uploads/2014/02/207632499-Pb-Class-Size.pdf.

62. *See* Joey Garrison, *Haslam Signs Bill Undoing Controversial Teacher License Policy*, THE TENNESSEAN (Apr. 25, 2014, 9:43 AM), http://www.tennessean.com/story/news/education/2014/04/24/haslam-signs-bill-undoing-controversial-teacher-license-policy/8121885/.

63. RITA KRAMER, ED SCHOOL FOLLIES: THE MISEDUCATION OF AMERICA'S TEACHERS (2001).

64. *See* George Leef, *A Key Reason Why American Students Do Poorly*, FORBES (Oct. 24, 2013, 12:14 PM), http://www.forbes.com/sites/georgeleef/2013/10/24/a-key-reason-why-american-students-do-poorly/.

stigmatize teachers who are dealing with challenging student bodies and scarce resources. They posit that, since teachers are the ones who best know what is going on in their classrooms, they should be the main actors making major decisions about students' education. They lament the trend toward subjecting teachers to outside control, a major goal of school reform policies over the past century.[65]

As is often the case, the best solution to these problems may lay somewhere in between these polarized views. There is little doubt that the nation has underinvested in and undervalued the work of teachers, particularly in high poverty communities. At the same time, expectations for student learning are higher today, and the diversity of student backgrounds and their needs have dramatically grown. Surely, technology and data are not a silver bullet, but they are part of the solution for supporting, empowering, and further professionalizing teachers. In fact, in many charter schools and teacher-led schools, rather than technology and data being forced upon teachers, it is teachers who are gravitating toward them as an important part of their instructional toolbox.

C. Hard Lessons

The use of data analysis for measurement and improvement of school, teacher, and student performance inevitably exposes truths that may be uncomfortable to some but of great service to others.[66] Such is the nature of cold hard facts. For instance, schools in wealthy neighborhoods that have traditionally been prestigious may turn out to be less desirable when compared to competing schools from less privileged locales. The analysis may reveal that public charter schools underperform their non-charter public counterparts, thus attracting students for non-education related reasons.[67] Programs funded by taxpayers' money may be proven ineffective. The success of graduates of leading academic institutions may be linked more closely to preexisting social status than to academic achievement. Parents may

---

65. JAL MEHTA, THE ALLURE OF ORDER: HIGH HOPES, DASHED EXPECTATIONS, AND THE TROUBLED QUEST TO REMAKE AMERICAN SCHOOLING (2013); *see also* Leonie Haimson, *The Reality and the Hype Behind Online Learning and the 'School of One'*, HUFF. POST (Sept. 7, 2012, 12:22 PM), http://www.huffingtonpost.com/leonie-haimson/the-reality-and-the-hype-_b_1859859.html.

66. *See* INST. FOR A COMPETITIVE WORKFORCE, NAT'L CHAMBER FOUND., U.S. CHAMBER OF COMMERCE, THE UGLY TRUTH: A STATE-BY-STATE SNAPSHOT OF EDUCATION IN AMERICA (2011), *available at* http://www.uschamberfoundation.org/sites/default/files/publication/edu/The%20Ugly%20Truth.pdf.

67. *See* Tim Post, *Bill Targets Underperforming Minn. Charter Schools*, MPR NEWS (Feb. 10, 2014), http://www.mprnews.org/story/2014/02/09/proposed-bill-would-subject-charter-schools-to-more-scrutiny.

be appalled to learn that their children are not performing as well as they thought compared to their peers in the state, country, or worldwide. In sum, data analysis can unearth discreet discrimination, concealed incompetence, pockets of neglect, and excess capacity.

These lessons may be unpleasant but necessary to learn. Consider a report by the National Center for Education Statistics, which showed that despite comprising 15 percent of all college students in the United States (and 13.1 percent of the general population) in 2009, African-Americans obtained just 7 percent of the nation's science, technology, engineering and mathematics (STEM) bachelor's degrees, 4 percent of master's degrees, and 2 percent of PhDs.[68] The Report further shows that even when they have earned all of those degrees, African American scientists attracted markedly less funding than their white counterparts.[69]

Or consider that with the help of student data tracking, New York City learned in 2013 that almost four out of five public high school graduates needed remediation when they entered city community colleges. Naturally, this suggested a mismatch between the content of state high school tests and the information needed to succeed in college.[70] According to another recent report, *Building A GradNation: Progress and Challenge in Ending the High School Dropout Epidemic*, fewer than one in four students with disabilities earns a high school diploma in Nevada, compared to 81 percent in Montana.[71] Further, the Report shows that in Minnesota, just 59 percent of low-income students graduate compared with 87 percent of their wealthier peers. Such striking disparities, which surface as a result of data analysis, help school districts, states, and the federal government craft appropriate policy responses.

But, as previously mentioned, these studies and the statistics behind them have their critics too. Teacher unions fear that big data strategies mask a hidden agenda of culling the herd, replacing properly trained teachers with less qualified employees, or possibly

---

68. Liana Christin Landivar, *Disparities in STEM Employment by Sex, Race and Hispanic Origin*, AM. COMMUNITY SURVEY REPORTS (Sept. 2013), http://www.census.gov/prod/2013pubs/acs-24.pdf.

69. Donna K. Ginther et al., *Race, Ethnicity, and NIH Research Awards*, 333 SCI. 1015 (2011), *available at* http://www.sciencemag.org/content/333/6045/1015.full.

70. *See* Anya Kamenetz, *What Parents Need to Know About Big Data and Student Privacy*, NPR (Apr. 28, 2014, 11:58 AM), http://www.npr.org/blogs/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy.

71. ROBERT BALFANZ ET AL., BUILDING A GRAD NATION: PROGRESS AND CHALLENGE IN ENDING THE HIGH SCHOOL DROPOUT EPIDEMIC, ANNUAL UPDATE 4 (Apr. 2014), *available at* http://gradnation.org/sites/default/files/17548_BGN_Report_FinalFULL_5.2.14.pdf.

just technology.[72] And parents are concerned about the aggregation of children's data, its persistence over time, and its potential monetization by vendors. Others worry that the benefits of big data analysis will disproportionately accrue to the rich and the powerful, who are often better equipped to make use of digital resources. As Seeta Gangadharan observes, "[T]he underserved have less opportunity to take part in 'good surveillance' projects. As late adopters of new technologies, poor people find themselves excluded from certain kinds of data flows."[73] Thus, big data may accentuate an already deepening technological divide.

While the broader societal debate around the role of technology and data in education will continue to occupy policymakers for years to come, this discussion transcends privacy concerns. It implicates larger policy choices about measurement and standardization, centralized (federal) or distributed (state and district) control over K–12 education, resource allocation, digital literacy, and equality. In order to better address specific, current educational privacy concerns, these issues must be disentangled from broader scope ed tech societal debates and considered separately on their own merits.

IV. TECHNICAL PRIVACY CHALLENGES

Some of the true privacy challenges that have arisen with the emergence of ed tech are common to those frequently raised in other market segments and industries. They include concerns about outsourcing, vendor contracts, data security, and compliance with fundamental privacy principles. These concerns 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.

This Part lays out traditional privacy concerns that arise in the context of ed tech deployment and segregates them from the other education policy challenges discussed in the previous Part. It begins by cataloging the issues raised by the influx of technology vendors into the school environment. It continues with a comprehensive overview

---

72. *See Education Technology Catching on at Last*, ECONOMIST, June 29, 2013, http://www.economist.com/news/briefing/21580136-new-technology-poised-disrupt-americas-schools-and-then-worlds-catching-last.

73. Seeta Gangadharan, *Knowing Is Half the Battle: Combating Big Data's Dark Side Through Data Literacy*, SLATE (Apr. 2, 2014, 10:13 AM), http://www.slate.com/blogs/future_tense/2014/04/02/white_house_big_data_and_privacy_review_we_need_federal_policy_about_digital.html; *see also* SEETA PEÑA GANGADHARAN, NEW AM. FOUNDATION, JOINING THE SURVEILLANCE SOCIETY? NEW INTERNET USERS IN AN AGE OF TRACKING (Sept. 2013), *available at* http://newamerica.net/sites/newamerica.net/files/policydocs/JoiningtheSurveillanceSociety_1.pdf.

of the regulatory terrain, including a discussion of the Family Educational Rights and Privacy Act (FERPA),[74] its shortcomings, and a critique of brewing legislative responses. Finally, it proposes that to address the flaws in the current framework, both educational institutions and private sector vendors must engender public trust and strengthen data governance mechanisms.

A. Commercialization

Education is not the first sector where businesses have driven an agenda of reform and data innovation. Yet in education, public emotions are stoked by the specter of children exposed to commercial forces at a tender age. And given these sensitivities, differences of opinion about seemingly technical issues can flare into politically fraught controversies among government officials, teacher unions, parents and industry groups.

More generally, some critics are 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. They posit 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. With a K–12 education system that is provided primarily by unionized teachers in the public sector, new educational models are the source of heated opposition.

This section discusses the policy concerns and existing regulatory responses related to commercialization in the sphere of public education.

1. Commercial Use and Marketing

The debate over commercial activities in schools is decades old.[75] Schools have long had policies to determine the legitimacy of commercial activities including billboards in sports fields, vending machines in cafeterias, outsourced yearbooks, and even ads and branding on textbooks and core education products. This ongoing

74. 20 U.S.C. § 1232g (2012).

75. *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 (2014), *available at* http://nepc.colorado.edu/files/trends-2013.pdf.

debate is now converging with the heated discussion surrounding commercial use of student data.[76]

According to a January 2014 survey by Common Sense Media, 86 percent of 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."[77] Given the perception, regardless of its truth, that a business offering a free service must intend to monetize its data, services such as email and document sharing that are offered to educational institutions for free automatically raise privacy and data security concerns. Further contributing to these concerns, free products and services typically do not go through a formal procurement process where professionals evaluate regulatory compliance and privacy risks.[78]

MOOCs too have come under close scrutiny for existing or potential future data monetization.[79] And 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."[80] In reality, however, although inBloom's model did allow for data to be shared with vendors, this was largely at the discretion of school districts and intended to streamline their ability to integrate third-party applications of their choice.

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 online school newspapers or yearbooks. 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

---

76. Anita L. Allen, *Minor Distractions: Children, Privacy and e-Commerce*, 38 HOUS. L. REV. 751, 754 (2001).

77. *Student Privacy Survey*, COMMON SENSE MEDIA, http://cdn2-d7.ec.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf (last visited Apr. 17, 2015).

78. Steve Mutkoski, *Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 511, 517 (2014) ("Teachers should understand that they may not bind the school (or students) to the provider's terms of service without formal review.").

79. *See* Watters, *supra* note 30.

80. 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 (internal quotation marks omitted).

may be restricted as a result of anti-marketing sentiments, they often implicate neither student privacy nor information privacy laws.[81]

Second, vendors may use student information to enhance and improve existing products and services or to develop related products and services; this may entail improving the same products and services sold to the students' school, improving other education products and services, or improving other non-education products and services. FERPA would bar the use of students' personally identifiable information for purposes that do not further the school's mission, but other non-covered student data could be used to improve a vendor's non-school related services. Hence, when analyzing commercial use, it is important to keep in mind two dimensions of the issue—the *type* of data, and the *use* of such data. Use of students' personally identifiable information for product improvement remains contentious, given that some vendors have a broad sweep of activities that are unrelated to the services they offer schools. Indeed, some proposed state bills would prohibit *uses* of data for both educational and non-educational purposes—regardless of the *type* of data—to the consternation of vendors, who believe that certain commercial activity in this vein is both appropriate and necessary to serve their customer base.

Third, vendors may use students' information to "market" or "advertise" new education products or services—for example, by recommending a level two math app after a student completes level one—to the students themselves, their families, and their teachers. This area also remains a subject of intense debate and requires further unpacking, as opportunities to customize learning intersect with concerns around commercial activity. Some argue that any form of marketing to kids should be banned, regardless of the nature of the products. Others say that students and families already use many third-party technologies at home but do so without sufficient nexus to school activities. They claim that in these situations, recommendation engines can empower families by providing them with information to help their children more effectively outside of school. In addition, they claim that vendor recommendations can help educators identify other services and resources offered by a primary vendor or its partners that meet their student or school needs. Finally, delineating the boundary

81. In this respect, the Student Online Personal Information Protection Act (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), *available at* 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. *See id.*

of appropriate use requires more nuance around the type of data accessed by vendors. For example, some recommendation engines do not require access to or sharing of personally identifiable information, but are based instead on metadata that match up a student's 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 primary educational purpose or selling their information to third parties. Unlike many of the other issues, there is wide agreement that these uses are inappropriate.[82] While such practices would in most cases violate FERPA and the Children's Online Privacy Protection Act (COPPA),[83] critics argue that statutory restrictions are quite narrow in scope. This could, for example, enable vendors to transact in information deemed not personally identifiable—but still collected from students in an educational setting—or to use data collected from children who have crossed the COPPA threshold of age thirteen, but are still minors.

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 considered commercial, behavioral advertising by some, could 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 be permitted to feature a third-party app store for kids? And could such an app store be tailored to a 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 schools 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

82. *See* DOE ONLINE GUIDANCE, *supra* note 11, at exs. 2 and 4 ("Under FERPA, the provider may not use data about individual student preferences gleaned from scanning student content to target ads to individual students . . . because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights.").

83. 15 U.S.C. §§ 6501–6506 (2012).

and mobile services are offered through a "freemium" model, which requires no payment upfront, but proposes upsells or serving ads to users. For example, Microsoft designed "Bing for Schools" for use in a K–12 environment and, therefore, features no advertisements, refrains from mining users' search queries, and automatically filters out adult content. But the Bing Rewards program incentivizes students to use Bing search by rewarding their schools with free Surface tablets, arguably a commercial practice.[84] SafeGov has criticized Google Apps for Education for scanning and analyzing the content of student email and web interactions although it does not serve students with ads.[85] Google has now confirmed that it has ended this practice.[86]

In addition, numerous websites that provide education services serve cookies, including third-party cookies that could ostensibly be used to profile users. Khan Academy, a widely used 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.[87]

Obviously, even with the best of intentions, market players are struggling to correctly balance commercial interests with student privacy rights.

Reacting to the public outcry over alleged data improprieties, US Senator Ed Markey recently submitted a bill intended to amend FERPA "to ensure that student data handled by private companies is protected . . . ."[88] Under the bill, schools are prohibited from

---

84. *See* John Ribeiro, *Microsoft Opens Ad-Free Bing for Schools Search Engine to All U.S. Schools*, PCWORLD (Apr. 23, 2014, 7:09 AM), http://www.pcworld.com/article/2147200/bing-for-schools-out-of-pilot-stage-promises-adfree-search.html.

85. *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.

86. *See* Juan Carlos Perez, *Google Stops Scanning Gmail Messages for Ads in Apps for Education*, PCWORLD (Apr. 30, 2014, 10:25 AM), http://www.pcworld.com/article/2149960/google-stops-scanning-gmail-messages-for-ads-in-apps-for-education.html.

87. 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.

88. Protecting Student Privacy Act of 2014, S. 2690, 113th Congress (2014), *available at* http://www.markey.senate.gov/imo/media/doc/2014-07-14_StudentPriv_BillText.pdf.

"releasing, or otherwise knowingly providing access to personally identifiable information . . . in the education records of a student to advertise or market a product or service."[89] And in California, under the 2014 draft of the 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" would be prohibited.

2. Security

Both the sharing of schools' student data with third-party vendors and its eventual migration from local servers to the cloud inevitably raise concerns about privacy and data security. It is certainly essential that vendors providing service to schools offer first-rate 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.[90]

Some are concerned that cloud services, by their nature, create security risks. And, with data migrating from multiple schools via the web to a tech vendor's vault that is sometimes located in a foreign jurisdiction and accessible by multiple parties, how could they not? One commentator warned against outsourcing to companies that "are the subject of 20-year consent decrees for engaging in deceptive practices surrounding privacy and/or security," referring to the typical duration of a consent order issued by the FTC against some of the marquee cloud companies, including Microsoft and Google.[91] According to the CLIP Study, cloud vendor contracts often fail to impose data deletion requirements, which are, in fact, mandated in certain contexts under FERPA,[92] as well as security breach notification obligations. More specifically, the CLIP 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."[93]

---

89. *Id.*; *see also* David Nagel, *Student Data Not a 'Product' to Be 'Sold to the Highest Bidder'*, THE JOURNAL (Jan. 14, 2014), http://thejournal.com/articles/2014/01/14/student-data-not-a-product-to-be-sold-to-the-highest-bidder.aspx.

90. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

91. Hoofnagle, *supra* note 35.

92. *See* CLIP STUDY, *supra* note 8, at 31–32. For deletion obligations, *see, e.g.*, 20 U.S.C. § 1232g(b)(1)(F), (b)(3) (2012).

93. CLIP STUDY, *supra* note 8; *see also* Andrea Cascia, *Don't Lose Your Head In The Cloud: Cloud Computing And Directed Marketing Raise Student Privacy Issues In K–12 Schools*, 261 ED. LAW REP. 883, 889 (2011).

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 the avalanche of security alerts, security patches, and updates needed to keep data systems secure. In addition, proponents of a school-hosted system often ignore the fact that most schools already rely on remote servers for computing powers, and that, unlike banks or hospitals, schools could not possibly have the resources needed to independently host and administer their IT architecture.

The FTC has recently stressed the importance of exerting appropriate controls over vendors' data security practices in the matter of *GMR Transcription Services, Inc.*[94] While not in the context of education, *GMR* 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:

> [R]equire [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.[95]

Moreover, the FTC faulted GMR for not performing 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 for the agency to leverage its Section 5 jurisdiction to impose such security standards on school vendors absent a direct representation by those vendors to users of their service. Given this likely scenario, state legislation may be useful in requiring school vendors to provide appropriate security protections to the data they hold regardless of the existence of a user interface.

---

94. *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.

95. Complaint at 4, In the Matter of GMR Transcription Servs., Inc., No. C-4482, (FTC Aug. 21, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.

3. 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 even on 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 selling children's data to downright identity theft.[96] Yet, entrenching behind a "no vendor" model is no panacea, as schools are unlikely to have the wherewithal to carry the technological load. In fact, schools often turn to vendors as the *most secure* avenue for safeguarding student data. So instead, schools must implement appropriate data governance mechanisms to actively manage their information systems and relationships with vendors.

Privacy laws typically do not proscribe sharing personally identifiable information with vendors, so long as a vendor acts under the 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.[97] 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 multiple IT functions.[98] Indeed, reliance on vendors including cloud providers, IT consultants, transaction processors, and other business associates has become the industry norm.[99] Schools too need to engage a variety of experts to handle a broad range of tasks and such relationships

---

96. *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/.

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

98. *See Customer Success. Powered by the AWS Cloud*, AMAZON WEB SERVICES, https://aws.amazon.com/solutions/case-studies/?nc1=f_cc (last visited Apr. 17, 2015).

99. *See* Jan Hertzberg, *Managing Data Security and Privacy Risk of Third-Party Vendors*, GRANT THORTON 1 (Oct. 15, 2011), *available at* http://www.grantthornton.com/staticfiles/GTCom/Health%20care%20organizations/HC%20-%20managing%20data%20-%20FINAL.pdf.

inevitably entail sharing students' data. However, the term "sharing" is charged, as some assume that vendors are given direct access to children's data for open-ended goals. In fact, in many cases, "sharing" with a vendor involves using a vendor platform for school management of data, together with value-added services that reformat (dashboards), analyze (predictive analytics) or take action on (adaptive software algorithms) student information.

Some have proposed relying on parental consent as a solution for storing data in the cloud or enabling use of certain technologies. Parents should certainly be part of the technology planning discussion at schools and school districts through appropriate committees and consultation. But individual parents are ill-positioned 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 . . . ."[100] In addition, accommodating the technology choices of individual parents would force schools to operate multiple duplicative systems, an impossible task that would also leave some children without access to basic services that others receive, raising new concerns about equity.

Information privacy laws have traditionally carved out a category of trusted third parties who can, under certain restrictions, obtain data from first parties. The European Data Protection Directive, for example, distinguishes between "data controllers," who determine the purposes and means of data use, and "data processors," which operate at their behest.[101] While data controllers are subject to the full gamut of privacy laws, including the principles of

---

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

101. 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), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf. 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." *Key Definitions of the Data Protection Act*, ICO, http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions (last visited Apr. 17, 2015). "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.*

transparency, individual choice, subject access, and data minimization, processors are generally required to adhere to purpose limitation clauses and implement appropriate data security. Likewise, in the healthcare arena in the United States, 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."[102] 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,"[103] for purposes such as claims processing, quality assurance, billing, and data analysis or administration and more.[104] Similarly, 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.[105] However, a financial institution is authorized to share data with service providers operating to perform services for it or to function on its behalf, which includes marketing its 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, US 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. In sum, allowing individuals to opt-out of having their information shared with vendors

---

102. *See* 45 C.F.R. § 160.102 (2014). Protected health information (PHI) under HIPAA consists of all "individually identifiable health information." 45 C.F.R. § 160.103 (2014).

103. *See* 45 C.F.R. § 164.502 (2014).

104. 45 C.F.R. § 160.103 (2014). 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." U.S. Dep't of Health & Human Servs., *Business Associates*, HHS.GOV, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last revised Apr. 3, 2003). Furthermore, any disclosed information may not be used for the business associate's independent use or purposes. *See id.* 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.

105. *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.

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.

B. Outdated Regulatory Terrain

Despite—or perhaps because of—the significant current and historical interest in protecting student privacy, the regulatory regime designed to protect students' personally identifiable information is a patchy collage of federal and state laws and regulatory guidance. While FERPA rightfully dominates discussions of student data, parents, students, educators, and vendors must also navigate COPPA, the Protection of Pupil Rights Amendment (PPRA),[106] numerous state laws, and a web of product and service-specific contracts. Understanding how FERPA, COPPA, and the PPRA have developed to address data collection and sharing by schools is critical to charting a path to address new policy concerns.

1. FERPA

Before the passage of FERPA in 1974, it was not clear which parties could access and share student data and what rights, if any, parents had in their children's information. School newspapers and the general media published information about students who made various sports teams, including such students' height and weight. Hometown newspapers proudly featured lists of graduates, as well as the names of students who made the honor roll or won awards. The names of winners of the Westinghouse Science Talent Search were broadcast on the radio. School yearbooks published information about students, including names, photos, and various personal details. Parents who volunteer at schools could even access sensitive information about students other than their own child. Hence, a broad range of student data was collected, shared, and often made public.

The rules about 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 inaccurate or stigmatizing information.

In the early 1970s, 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

106. 20 U.S.C. § 1232h (2012).

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."[107] This concern about secret files both frames and underlies the mechanism introduced by FERPA, but also forewarns its shortcomings.

a. FERPA Fundamentals

In 1974, a mere twelve days after President Richard Nixon's resignation, the Buckley Amendment, known today as FERPA, was signed into law by Nixon's successor, President Gerald Ford.[108] 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.[109] Accordingly, the sole sanction under FERPA is the withdrawal of federal funding by the Department of Education. FERPA had two main goals: First, it allowed parents 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."[110]

For purposes of this discussion, it is critical to understand the development of three fundamental aspects of the FERPA regime: what constitutes education records; which disclosures are or are not permitted; and, in particular, what is the scope of the "school officials" exception. Tracing the evolution of commercial entities' access to student information through these vectors exposes the growing gap between modern educational practices and the 1974 law that still governs them.

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

---

107. STUDENT PRESS L. CTR., WHITE PAPER: FERPA AND ACCESS TO PUBLIC RECORDS 5 (2010), http://www.splc.org/pdf/ferpa_wp.pdf (alteration in original).

108. *See* U.S. DEP'T OF EDUC., LEGISLATIVE HISTORY OF MAJOR FERPA PROVISIONS 1 (June 2002), *available at* http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpaleghistory.pdf.

109. 34 C.F.R. § 99.1 (2014). 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) (2012).

110. *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 38, 39 (Marci Kanstoroom & Eric Osberg, eds., 2008).

acting for the agency or institution."[111] This definition suggests that FERPA only protects those documents affirmatively kept or collected by a school.[112] 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.[113] 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.[114]

The Court's narrow, formalistic approach is quite inapposite to the general conception of personally identifiable information in privacy regulation as any information about an identified or identifiable individual.[115] Indeed, experts argue that even the term "personally identifiable information" has reached its zenith, given the ability to harness apparently *unidentifiable* information to track individuals. To be sure, FERPA *also* introduces the term personally identifiable information, prohibiting educational entities from releasing or providing access to "any personally identifiable information in education records."[116] FERPA defines personally

---

111. 20 U.S.C. § 1232g(a)(4)(A) (2012); *see also* 34 C.F.R. § 99.3 (2014) (definition of "education record"). Contrast this to the definition of the term "record" in the Privacy Act, 1974, enacted just a few months after 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) (2012).

112. *See* 20 U.S.C. § 1232g(a)(4)(A).

113. Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. 426 (2002); *see* Daniel R. Dinger, *Johnny Saw My Test Score, So I'm Suing My Teacher,* Falvo v. Owasso School District*, Peer Grading, and a Student's Right to Privacy Under the Family Education Rights and Privacy Act*, 30 J.L. & EDUC. 575 (2001); Randi M. Rothberg, *Not as Simple as Learning the ABC's: A Comment on* Owasso Independent School District No. I-011 v. Falvo *and the State of the Family Educational Rights and Privacy Act*, 9 CARDOZO WOMEN'S L.J. 27 (2002).

114. *Id.* at 433; *see also* Jensen v. Reeves, 3 Fed. App'x 905, 910 (10th Cir. 2001)*;* Lynn M. Daggett, *FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students*, 58 CATH. U. L. REV. 59, 72 (2008).

115. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

116. 20 U.S.C. § 1232g(b)(2) (2012). While FERPA does not define personally identifiable information, a federal regulation issued thereunder does. *See* 34 C.F.R. § 99.3 (2014) (defining personally identifiable information as a student's name; address; personal identifier, such as a

identifiable information to include: (a) direct identifiers (such as a student's or other family member's name) and (b) indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name), as well as (c) a catch-all category capturing "[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 . . . to identify the student with reasonable certainty."[117]

However, as Solove and Schwartz point out, despite mentioning personally identifiable information, FERPA's central purpose remains that of "education records."[118] 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' personally identifiable information.[119] And although, notwithstanding *Owasso*, schools and vendors generally treat students' personally identifiable information of any sort as subject to privacy protections, the term "education records" remains ill-suited to anchor privacy protection in a big data world.[120] 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.

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.[121] Schools typically

---

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.").

117. 34 C.F.R. § 99.3 (2014) (defining "personally identifiable information").

118. *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.

119. 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.

120. *See* Robert W. Futhey, Note, *The Family Educational Rights & Privacy Act of 1974: Recommendations for Realigning Educational Privacy with Congress' Original Intent*, 41 CREIGHTON L. REV. 277, 297–308 (2008).

121. 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

use the directory information exception to publish yearbooks, phone directories, concert programs, sports teams' rosters, and the like. In addition, FERPA authorizes disclosure without parental consent or opt-out rights 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.[122] Finally, to prevent circumvention of its purpose limitation rules, FERPA prohibits re-disclosure of student personally identifiable information pursuant to an authorized disclosure.[123] Consequently, if a school shares student data with a vendor under the "school official" exemption, that vendor may share the data with another vendor only as long as the data are used for the same purpose, e.g., provision of the same service, set forth by the school.[124]

Similar to HIPAA, GLBA, and the European Data Protection Directive, FERPA recognizes data sharing with certain third parties. FERPA allows schools to share students' personally identifiable information 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."[125] 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.[126] Hence, merely identifying

---

received, and the most recent education agency or institution attended by the student." 20 U.S.C. § 1232g(a)(5)(A) (2012); *see also* 34 C.F.R. § 99.3 (2012).

122. *See* 20 U.S.C. § 1232g(b)(1)(A)–(F) (2012).

123. *See id.* § 1232g(b)(4)(B); 34 C.F.R. § 99.33 (2014).

124. Kathleen Styles, the chief privacy officer of the US 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.

125. 20 U.S.C. § 1232g(b)(1). 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.

126. 34 CFR § 99.31(a)(1)(i) (2014).

an entity as a "school official" does not provide it with carte blanche access to or use of education records.[127]

School officials include contractors, consultants, and even volunteers to whom a school has outsourced institutional services or functions.[128] As a result, vendors such as school tutors, cafeteria and busing services, and attorneys and information technology providers are regularly classified as school officials so schools can share data with them. While the terminology is confusing, 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. Until the FERPA amendments of 2009, it was not clear that vendors could be designated "school officials" at all, creating a roadblock for many services that are now commonplace.

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

The US Department of Education recognizes the necessity of employing 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.[129]

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 FERPA."[130]

Under FERPA, a "school official" is restricted to using student records for only a "legitimate educational interest." As the Department of Education makes clear, with the exception of that student information that has been properly de-identified or that is shared under the "directory information" exception:

---

127. *See Defining "Legitimate Educational Interests,"* NAT'L CTR. FOR EDUC. STATS, http://nces.ed.gov/pubs2004/privacy/section_4b.asp (last visited Apr. 17, 2015).

128. *See id.*

129. DOE ONLINE GUIDANCE, *supra* note 11.

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

> If the school or district has shared information under FERPA's school official exception . . . the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed . . . (*i.e.*, to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII [personally identifiable information] by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.[131]

Responding to a line of questions by Senator Markey, the Department of Education has recently explained its interpretation of FERPA's school official exemption in the context of product development. The Secretary of Education stated that:

> [T]he contractor could use FERPA-protected information to improve the products the school or district was using . . . . However, FERPA would not allow [a] contractor to use the FERPA-protected data to create a product never intended for use by the school or district. Similarly, FERPA would not permit a school or district to give FERPA-protected data to a third party solely for it to develop a product to market to a school or district.[132]

These restrictions were reinforced by a set of best practices issued by the Software & Information Industry Association (SIIA), which provide that "[s]chool service providers collect, use, or share student [personally identifiable information] only for educational and related purposes for which they were engaged or directed by the educational institution, in accordance with applicable state and federal laws."[133]

To help flesh out legitimate uses of student data for product improvement, the Department of Education provided several examples in its recent Online Guidance. In one example, a vendor that provides a school district with an online tutoring and teaching program collects metadata about student activity, including time spent online, desktop versus mobile access, success rates, and keystroke information. The Department of Education states that, if the vendor de-identifies the data, it can use the information to develop new personalized learning products and services—unless the district's agreement with the

---

131. DOE ONLINE GUIDANCE, *supra* note 11.

132. Letter from Arne Duncan, Sec'y of Educ., *supra* note 130.

133. SOFTWARE & INFO. INDUSTRY ASS'N, BEST PRACTICES FOR THE SAFEGUARDING OF STUDENT INFORMATION PRIVACY AND SECURITY FOR PROVIDERS OF SCHOOL SERVICES (Feb. 24, 2014). Kathleen Styles, the chief privacy officer of the Department of Education, explained:

> For instance, the school or district could also require the provider to develop products for the school or district to use with its students. During the course of providing those services, the cloud provider could use FERPA-protected information to improve the products the school or district was using. FERPA would permit the school or district to include provisions like this in its contract with the cloud provider. On the other hand, FERPA would not allow a cloud provider to use protected data to create a product never intended for use by the school or district.

Solove, *supra* note 124.

vendor precludes this use.[134] Under another example, a vendor that contracts with a school district under the school official exception to provide basic productivity applications may not use data about individual student preferences to target ads to those students, since "using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights."[135] However, it is unclear to what degree "target ads" equate to adaptive educational engines that recommend learning resources that best address student needs.

FERPA mandates that personally identifiable information from educational records shared with a vendor must remain "under the direct control of the school or district with respect to the use and maintenance of education records."[136] This means that when a school shares student data with a technology vendor, the parties must set forth the privacy and data security obligations for the vendor in a contract. Alas, according to the CLIP Study, the contracts of schools with service providers typically lack measures, which are characteristic of vendor contracts in other industry sectors, such as security requirements, security breach obligations, and indemnification and liability provisions.[137]

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-to-accept agreements. Typically, neither schools and teachers nor small technology vendors have the incentive to negotiate such contracts, which sometimes do not provide comprehensive FERPA commitments and allow vendors to unilaterally change the terms of the deal. The Department of Education stresses that "[e]xtra caution and extra steps are warranted before employing click-wrap consumer apps."[138] This does not imply, of course, that click-wrap is inherently deficient. It is impractical to think that every school would negotiate standard contracts with every vendor. Rather, the point is that, when used in the education arena, click-wrap contracts need to transparently and satisfactorily address

134. DOE ONLINE GUIDANCE, *supra* note 11, at ex. 1.

135. *Id.* at ex. 4.

136. 34 C.F.R. § 99.31(a)(1)(i)(B)(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." DOE ONLINE GUIDANCE, *supra* note 11.

137. CLIP STUDY, *supra* note 8.

138. DOE ONLINE GUIDANCE, *supra* note 11.

at least the minimum requirements of applicable education privacy laws.

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

b. FERPA Shortcomings

Critics point out many shortcomings of the FERPA regime.[139] To start, FERPA lacks an effective enforcement mechanism because it offers no avenue for individual redress[140] and gives the Department of Education no 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."[141] FERPA also limits the Department of Education's enforcement power over schools rather than downstream vendors. Thus, in the absence of a private cause of action, once student data leaves the hands of a school, it is no longer subject to a credible FERPA enforcement threat.[142]

It is important to note, however, that the Department of Education has somewhat greater enforcement leeway than critics have allowed. In some cases, the Department of Education can ban an individual vendor from doing business with schools for five years. Further, it can issue cease and desist orders and negotiate compliance agreements. And in *United States v. Miami University*, the court found that FERPA expressly permits the Secretary of Education to

---

139. Dan Solove called FERPA "old and ineffective," arguing that the federal statute was "in dire need of reform, as demonstrated by its failure to address so many key issues regarding the use of cloud computing services by schools and educational entities." 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. 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." *Id.*

140. Gonzaga Univ. v. Doe, 536 U.S. 273 (2002) (holding FERPA creates no personal rights enforceable through federal lawsuits); *see* Futhey, *supra* note 120.

141. Solove, *supra* note 139; *see also* Lynn M. Daggett & Dixie Snow Huefner, *Recognizing Schools' Legitimate Educational Interests: Rethinking FERPA's Approach to the Confidentiality of Student Discipline and Classroom Records*, 51 AM. U. L. REV. 1, 11 n.60 (2001).

142. *See* Daniel Solove, *Big Data and Our Children's Future: On Reforming FERPA*, LINKEDIN (May 7, 2014), https://www.linkedin.com/today/post/article/20140507051528-2259773-big-data-and-our-children-s-future-on-reforming-ferpa.

bring suit to enforce FERPA conditions in lieu of its administrative remedies.[143] In addition, the Department of Education's Privacy Technical Assistance Center has been proactive in crafting detailed guidance to dispel some of the interpretative ambiguity surrounding key statutory terms.[144] But given the historic lack of enforcement in this area, the concerns about enforcement shortcomings of FERPA resonate.

Secondly, FERPA's lack of a "vendor" concept in combination with the current organizational imperative to outsource non-core functions to third-party service providers, led to an amendment to the FERPA regulations in 2009, expanding the scope of the "school official" exception to include contractors, consultants, volunteers, and other outside parties to whom an educational agency has outsourced institutional services that it would otherwise use employees to perform.[145] 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 terminologically awkward category of "school officials."

A third issue is that FERPA provides little to no guidance about data governance and security obligations. Apparently, vendors are not required to develop a data breach response plan, much less a comprehensive privacy and data security program that is audited and enforced by an education institution—although state security breach notification laws may incentivize such actions for risk mitigation. These shortcomings compound the definitional issues discussed above,[146] such as FERPA's limiting focus on the term "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 right of parents to review and amend their children's education records. These rights reside with the parents until a student turns eighteen years old or enters a post-secondary institution, at which point they transfer from the parents to the student. In the past, such records typically contained a student's transcript as well as assessments by teachers. But the revolution in data collection and storage capabilities has facilitated access by

143. United States v. Miami Univ., 294 F.3d 797 (6th Cir. 2002).

144. *See, e.g.*, DOE ONLINE GUIDANCE, *supra* note 11; PRIVACY TECHNICAL ASSISTANCE CTR., U.S. DEP'T OF EDUC., FERPA EXCEPTIONS—SUMMARY (Apr. 2014), *available at* http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf.

145. C.F.R. § 99.31(a)(1)(i)(B) (2014).

146. *See supra* Part IV.A.2.

parents to information that is both more comprehensive and more granular. For example, school records may contain sensitive 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 their privacy against parental access to their information.[147] Indeed, Danah Boyd and Alice Marwick have cogently argued that teens are primarily concerned about surveillance by their parents.[148] 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.[149]

FERPA's limitations on disclosure of student data to third parties, while reasonable on its face, can also run counter to the public interest. Some of the information locked down in school coffers 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: "[D]ocuments included striking data on racial inequities. For example, African-American students represent only 15 percent of public school students, but they make of [sic] 35 percent of students suspended once, 44 percent of those suspended more than once and 36 percent of those expelled."[150] There is a compelling public interest to ensure the continued flow of such information.[151]

---

147. Stuart, *supra* note 39, at 1162–69.

148. Danah Boyd & Alice E. Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies (unpublished manuscript) (Sept. 2011), http://www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf (presented at *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society* at Oxford University).

149. 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.

150. *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.

151. Critics argue that rather than to protect children's privacy, schools use FERPA as a shield against disclosing unfavorable information to outside stakeholders. Mary Margaret Penrose wrote, "For years, schools have been hiding behind FERPA and intentionally preventing disclosure of records to third parties . . . . " Penrose, *supra* note 119, at 96; *see also* Matthew R. Salzwedel, *Cleaning Up Buckley: How the Family Educational Rights and Privacy Act Shields Academic Corruption in College Athletics*, 2003 WIS. L. REV. 1053 (2003); Nancy Tribbensee, *Privacy and Confidentiality: Balancing Student Rights and Campus Safety*, 34 J.C. & U.L. 393 (2008). 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." Jill Riepenhoff & Todd Jones, *Secrecy 101: College Athletic*

2. COPPA

In cases involving children under the age thirteen, student personally identifiable information is also covered by COPPA, which requires commercial companies to obtain express parental consent before collecting children's information online. COPPA applies to commercial websites, online services directed at children, and websites and services that have actual knowledge that they have collected personal information from children. Under COPPA, consent for a third-party collection of data may be obtained by a school in place of a parent, but only for use of data for school purposes and for no other commercial purpose. If, however, a vendor intends to use or disclose children's personally identifiable information for commercial purposes in addition to the provision of services to the school, it must obtain parental consent. The FTC views the use of students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service, as unrelated commercial activities thereby requiring parental consent.[152] Thus, any use in connection with online behavioral advertising or the like requires parental consent.[153]

In addition, in language recently introduced in its 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 a teacher, for example."[154] 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. As a result, many operators serving students in schools opt for gaining explicit parental consent rather than relying on schools for such consent. Schools are often asked to coordinate, but parents ultimately express consent directly to the operator.

Interestingly, the FTC suggests that "as a best practice," it should be schools or school districts, and *not individual teachers*, who

---

Departments Use Vague Law to Keep Public Records from Being Seen, COLUMBUS DISPATCH (May 31, 2009, 10:41 AM), http://www.dispatch.com/content/stories/local/2010/10/14/secrecy-redirect.html.

152. *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 Apr. 17, 2015).

153. *See id.*

154. *Id.*

should decide whether to engage a particular vendor's site or service. This best practice apparently aims to ensure appropriate vetting, which teachers may have neither the time nor expertise to perform 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."[155]

The overall effect of this guidance is that a teacher who identifies an online resource or an app they wish to use 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., the Houston school district software rating for parents.[156] Other teachers may not be aware of these obligations and continue to use the tools they deem most useful for their classroom, regardless of the existence of pre-approved school lists. Consequently, it is important that schools and school districts have established policies and practices in place, including training for teachers and other staff, who have the responsibility to vet websites and apps that collect or host student information.

Current COPPA practice has led many vendors to seek ways to avoid having to navigate the treacherous waters of the parental verification process. Some, for example, declare that their products are intended solely for individuals over thirteen years of age. But regrettably, parents will help their children lie about their age to enable them to use popular email services, social networks, video sites, and app stores.[157] At the end of the day, in its current incarnation, COPPA is failing to block access of determined children and youths to desired web services. Instead, it unwittingly serves as an incentive for general web services to provide more privacy friendly versions of their services to children, lest they be characterized as targeting kids and subjected to a heavy regulatory load.

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 to students, teachers, and schools. While the FTC has taken steps in this direction, allowing safe harbor programs to approve new age-verification technologies and approving new methods directly, it continues to limit some of the most widely used age-verification

155. *Id.*

156. *Software Ratings for Parents*, HOUSTON INDEP. SCHOOL DIST., http://www.houstonisd.org/Page/109830 (last updated May 5, 2014).

157. Larry Magid, *Survey: Many Parents Help Kids Lie to Get on Facebook*, CNET, Nov. 1, 2011, http://www.cnet.com/news/survey-many-parents-help-kids-lie-to-get-on-facebook/.

mechanisms, such as the use of credit card verified app store accounts.[158]

3. PPRA

Additional restrictions apply specifically to school and third-party use of student information for *marketing* purposes. Under the Protection of Pupil Rights Amendment (PPRA), a school district must notify parents in case of any collection, disclosure, use, or sale of student information for *marketing purposes* and give parents the opportunity to opt-out.[159] PPRA also requires school districts to develop and adopt policies, in consultation with parents, about any such commercial activities.[160] However, PPRA provides an exception for "the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions."[161] Such activities require neither parental notice and opt-out nor the development and adoption of policies under the PPRA.

The scope of application of FERPA and PPRA may or may not overlap. While FERPA protects student information from education records *maintained by a school or district*, PPRA (like COPPA) is invoked when personal information is *collected from a student*. The use of online educational services, for example, may give rise to situations where a school or district provides FERPA-protected data to open accounts for students, while PPRA applies to subsequent information gathered through a student's interaction with the online educational service.

4. State Laws

In the absence of Congressional action[162] and in the face of accelerating technological change and rising public outcry, state

158. 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 percent of parents have never shared this information with their children (age 3–12), and only 4 percent did not require children to ask permission before purchasing or downloading free apps. *See 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/.

159. 20 U.S.C. § 1232h(c)(2)(C)(i) (2012).

160. 20 U.S.C. § 1232h(c)(1)(E); (c)(4)(A).

161. 20 U.S.C. § 1232h(c)(4)(A).

162. In July 2014, Senator Edward Markey introduced a bill to amend FERPA, which includes new restrictions on commercial uses of student data by vendors. Protecting Student Privacy Act of 2014, S. 2690, 113th Congress (2014), *available at* http://www.markey.senate.gov/

legislatures, including those in Louisiana,[163] Oklahoma,[164] and California[165] have weighed in with a flurry of legislative proposals. These laws attempt to close loopholes and perceived weaknesses in existing privacy regulation. Not surprisingly, given the political pressure to act expeditiously, they often end up reflecting legislative overreaction and presenting crude solutions at the price of creating new problems. A patchwork of state laws also poses a challenge to stakeholders operating across state lines to the degree there are differences in definitions (e.g., student data) and requirements (e.g., security standards and third-party uses).

For example, in the 2014 legislative session, the California state senate considered the adoption of SOPIPA, which would prohibit use of "a student's personal information for any commercial purpose, including, but not limited to advertising or profiling." Similar bills are pending in a number of other states. Unwittingly, SOPIPA could end up barring vendors from using information to improve education products and services, or even to make instructional recommendations to teachers and students based on student performance data. In doing so, it conflates legitimate uses of student data with concerns about marketing to students, specifically through behavioral advertising.[166] Vendors often have legitimate and non-privacy sensitive commercial needs for data use, such as the improvement of existing products. These disparate uses raise distinct policy concerns that cannot be addressed in one fell swoop.

Equally problematic is SOPIPA's definition of the term "personal information," which includes a long list of data items "related to a student" as well as "any aggregation or derivative thereof." The governance of even basic statistical data by information privacy legislation could limit useful analysis of student and school performance at a minimal price to student privacy. Language in other proposed bills would prohibit the creation of student profiles, although vendors may in fact be tasked with compiling educational profiles, or

---

imo/media/doc/2014-07-14_StudentPriv_BillText.pdf.; *see also* Benjamin Herold, *Draft Overhaul of Federal Student Privacy Law Released by U.S. Senators Markey, Hatch*, EDUC. WEEK (May 14, 2014, 1:08 PM), http://blogs.edweek.org/edweek/DigitalEducation/2014/05/draft_overhaul_of_federal_stud.html.

163. H.B. 946, 2014 Reg. Sess. (La. 2014), *available at* https://www.legis.la.gov/legis/BillInfo.aspx?i=224975.

164. H.R. 1989, 54th Leg., Reg. Sess. (Okla. 2013), *available at* http://webserver1.lsb.state.ok.us/cf_pdf/2013-14%20ENR/hB/HB1989%20ENR.PDF.

165. S. 1177, 2014 Reg. Sess. (Cal. 2014), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_bill_20140220_introduced.pdf.

166. The FTC has recently clarified that behavioral advertising to children is off limits. *Complying with COPPA, supra* note 152.

collection of sensitive information, although sensitive information may serve crucial educational and safety needs in schools.

In 2014, reacting to a tidal wave of public criticism, the New York legislature passed a statutory measure intended—quite indiscreetly—to take inBloom out of business in the state. The new law introduced odd terminology, such as a "data dashboard operator," intended to outlaw the activities of the student data aggregator.[167] Yet, such awkwardly phrased legislation will inevitably raise more questions than it answers. For example, should inBloom have been permitted to keep servicing New York schools had it not provided a data dashboard? And will cloud service providers have to refrain from offering such dashboards in New York lest they be chased out of the state? Is there anything inherently improper in providing a data dashboard? Paradoxically, in many other contexts, privacy advocates promote the introduction of data dashboards as a solution for enhancing transparency and user control.[168]

Under legislation recently proposed in Louisiana, except for a parent, teacher, or school principal, "no person or public or private entity shall be granted access to a public school computer system where any student information is stored unless authorized in writing by the student's parent or legal guardian."[169] In addition, the law prohibits the collection of *any* student personally identifiable information except for information required to provide educational services to students, which is contained in a student's cumulative record. Clearly, the astounding breadth of the language of these provisions could, if in fact enforced, impair the reasonable day-to-day operation of schools.

5. Legislative Gaps

The patchwork of US privacy laws generally, and education privacy laws in particular, is laden with gaps. The provision of

---

167. S. 5355, 2013 Reg. Sess. (N.Y. 2013), *available at* http://open.nysenate.gov/legislation/bill/S5355-2013. The new law defines "data dashboard" as:

> An electronic data system or hosted software application or applications that is designed to utilize data and information collected, stored, organized or aggregated by a [shared learning infrastructure service provider] and that is designed to provide, through a contract between a New York school district and a data dashboard operator, end users such as educators, students and their families with access to customized student information with the goal of supporting instruction and student learning.

Id.

168. The legislation would actually have allowed inBloom to provide its interoperable services in substantially the same manner as before, but by contracting with regional education boards in New York, rather than the central State Board of Education.

169. H.R. 946, 2014 Reg. Sess. (La. 2014), *available at* https://www.legis.la.gov/legis/BillInfo.aspx?i=224975.

education services by for-profit entities operating outside the purview of education privacy laws raises challenging 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 thirteen. To emphasize this point, Coursera, a leading MOOC provider, 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."[170] Other providers operating in this space use caution with respect to the nomenclature they use—for example, to designate "certificates" earned by "participants" as opposed to "degrees" awarded to "students."

Additional gaps may weaken even the little protection afforded under existing legislation. For example, under FERPA, any party may share de-identified data without consent for any purpose, arguably including behavioral advertising.[171] And while the Department of Education issued sophisticated guidance with respect to de-identification,[172] critics argue that when data is not irreversibly made anonymous, de-identified information could continue to present privacy risks. In addition, COPPA does not restrict the collection of data about children over the age of thirteen, leaving most high school students outside its protective umbrella.

Given a regulatory framework that has developed over decades, reflecting an older era's technologies and business practices, and heavily influenced by political conflicts, it is not surprising that student data has become a privacy quagmire for today's vendors, schools, teachers, and parents. While those same forces make radical legislative reform unlikely, modest changes to the current structure can boost public trust in commercial vendors and educational institutions alike.

C. Technical Privacy Solutions

Some of the privacy issues that arise in the field of education reflect similar concerns to those that played out in other contexts such as healthcare, finance, and e-government. They reflect the disruption

170. *Terms of Use*, COURSERA, https://www.coursera.org/about/terms (last revised Jan. 2, 2014).

171. 34 C.F.R. § 99.30 (2014).

172. Privacy Technical Assistance Ctr., *Data De-identification: An Overview of Basic Terms*, U.S. DEP'T OF EDUC., http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf (last visited Apr. 17, 2015).

of long-held views and traditions by new and innovative technologies and business models. They result, in part, from the sluggish adaptation of laws originating in the 1970s to a newly evolved techno-social reality. Contractual and data security arrangements with vendors must be tightened as school information routinely migrates to the cloud. The relevant parties must reach decisions concerning the scope of legitimate uses of student data, including whether parents, schools, localities, or state or federal government should make the decisions. Clearly, student personally identifiable information 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? Moreover, may vendors market education related products to students, families, and educators based on their previous interactions? Clarification of key terms, such as "education records" and "personally identifiable information," is necessary. In sum, lines need to be drawn in the sand with respect to de-identification.

This section suggests that to chart a path forward, it is important to recognize that simply tightening contractual controls cannot create stakeholder trust. At the same time, any organization with activity in the student data ecosystem must institute robust data governance mechanisms, including privacy training, appointment of privacy officers, model communications with parents, and de-identification tools.

1. Engendering Trust

Both school leaders and ed tech vendors should seek to empower teachers, parents, and students and bring them along for the technology ride. 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 as 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 transition to maximizing big data benefits while restricting privacy and civil liberty costs.

Trust cannot be established, however, simply by tightening IT contracts[173] or complying with the technicalities of FERPA and PPRA. Parents, students, and teachers will not pore over vendor contracts and will therefore not be satisfied with an additional rider or contract clause. As the President's Council of Advisors on Science and Technology recently remarked, "[o]nly in some fantasy world do users actually read these notices and understand their implications before

173. CLIP STUDY, *supra* note 8, at 27.

clicking to indicate their consent."[174] Instead, trust must be built by enhanced transparency into *data practices* not *data contracts*, demonstrating to parents, students, and teachers the benefits and promises of data use and assuaging the fears of abuse and commodification of student data. Hence, at the federal level, policymakers should develop model communications to help schools provide parents with information about how student data is used and protected. State or local education agencies could be required to publish information about complaints received under FERPA and PPRA, including their numbers and overall nature.

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 held by the Data Quality Campaign found that parents want to have meaningful access to information about their children, to see how they are doing in real time, to nurture their strengths, and to support them in their weaknesses. They are not incentivized to support 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. These solutions, which this Article refers to as data featurization and enhanced algorithmic transparency, are discussed further below.[175]

2. Stronger Data Governance

An important step toward enhancing trust entails the creation of internal organizational structures for sound data governance. Just as school districts would not think of putting school buses on the road with known, unmitigated safety issues, they should also refrain from experimenting with student data absent appropriate privacy safeguards. Dan Solove went so far as writing, "Any company trying to do business with K–12 schools where privacy is involved is like a company trying to build a world-class research facility in the middle of an untamed jungle. There is no privacy infrastructure in K-12 schools."[176]

As demonstrated by ample evidence from other industry sectors, laws and regulations are not enough; lofty principles on the books must be given life by a cadre of adequately trained and

---

174. WHITE HOUSE REPORT, *supra* note 4, at xi.

175. *Infra* notes 204–10 and accompanying text.

176. Daniel Solove, *Why Did inBloom Die? A Hard Lesson About Education Privacy*, SAFEGOV (Apr. 28, 2014), http://www.safegov.org/2014/4/28/why-did-inbloom-die-a-hard-lesson-about-education-privacy.

resourced professionals on the ground whose job it is to spot, identify, and mitigate privacy risks.[177] Few if any of the nation's fifteen thousand school districts have a role dedicated to managing student data privacy. Moreover, while school budgetary constraints are no doubt a factor, they can be mitigated through resourceful management strategies. For example, small districts could share a privacy role with neighboring districts while larger ones employ a full time privacy officer. At the very least, state education agencies should appoint dedicated privacy staff. Indeed, New York has recently created a chief student privacy officer at the state level to coordinate the protection of personally identifiable student data by local education agencies.

With appropriate privacy training, professionals in states and school districts would be able to spot issues arising from the deployment of new technologies in classrooms; create data classification schemes—not all student data are created equal in terms of identifiability and sensitivity; enact and oversee information security programs; and implement processes for ethical choices concerning innovative uses of student information.

The Department of Education can enhance its privacy engagement by tightening relationships with the privacy professional community. For example, it could set up a privacy advisory committee akin to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee or hire a privacy scholar-in-residence, similar to the role created by the FTC.

3. Vendor Management

In case after case, vendors have become the central focus of the privacy debate, even as decisions about data collection and use are in the hands of their customers, who interact directly with individual consumers. Carrier IQ, an analytics vendor serving telecom carriers that has no rights to use customers' data, became the focus of consumer debate when its data practices came to light.[178] Similarly, Euclid, a mobile analytics location company, was the source of controversy after the media aired Nordstrom's test of its new technology.[179] Likewise, inBloom was blasted for delivering the data agenda pursued by its customers—schools, school districts and state

177. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

178. Joe Brodkin, *Carrier IQ Hit With Privacy Lawsuits as More Security Researchers Weigh In*, ARS TECHNICA (Dec. 2, 2011, 4:49 PM), http://arstechnica.com/tech-policy/2011/12/carrier-iq-hit-with-privacy-lawsuits-as-more-security-researchers-weigh-in/.

179. Wendy Davis, *Senator Says Euclid's Location Tracking Fails Privacy Test*, MEDIA POST (Apr. 2, 2013), http://www.mediapost.com/publications/article/197185.

education departments—which had a strong interest in gaining control of their data by streamlining and simplifying their data architectures.

In this vein, Solove and Hartzog recently proposed expanding vendors' responsibilities under Section 5 of the FTC Act. Under their theory, the FTC's body of consent decrees establishes that "there is a standard of care when it comes to contracting" that might oblige private entities to protect students' privacy—or that might recognize students as third-party beneficiaries entitled to privacy protections during such deals. If that were the case, private sector vendors, subject to oversight by the FTC, would protect students' privacy interests even if schools' data governance remained inadequate.

At first blush, this appears to be an attractive solution. After all, why not impose responsibility on for-profit businesses that seek to access student data? Under closer scrutiny, however, calling for vendors to lead public education efforts around ed tech privacy is asking the tail to wag the dog. Such a call is based on a view of a market driven entirely by supply forces—vendors trying to market their goods–without proper accounting for the tremendous demand arising from ninety thousand schools and fifteen thousand school districts. Hence, the education system must become more sophisticated about its data practices from a technological, policy, and public relations perspective.

Education is not the first area where vendor relations must adapt to the needs of a regulated sector. Much like schools migrating data to the cloud, the federal government has had to overcome obstacles in order to contract for remote outsourcing solutions. In order to streamline contracting processes and set forth standard criteria for engaging vendors, the US Chief Information Officer (CIO) initiated an on-ramp process known as 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. Other regulated industries, including health care and finance, have worked to streamline contracting practices to accommodate cloud solutions. In healthcare, for example, Google has recently announced it would support HIPAA-compliant clouds, with Google Apps and Google Cloud Platform entering into business associate agreements to handle HIPAA-protected

information on behalf of a range of healthcare applications and technologies.[180]

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, unfortunately, the process will likely not be as seamless 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.

V. NEW PRIVACY CHALLENGES

Societal judgments about the education system and fissures in an outdated regulatory framework are not the only privacy-related concerns exposed by ed tech innovation. As big data and sophisticated "small data" tools and capabilities make their way into schools, educators are faced with new ethical challenges, including concerns over unfairness and discrimination in algorithmic decision making, narrowcasting and filter bubbles, predictive sorting, and the stratification of society into "haves" and "have nots." To pave a path forward, this Part suggests a new toolbox of solutions, including empowering parents through data "featurization" and algorithmic transparency in order to build trust into a system that relies on society's faith in teachers and schools. While implementing these solutions, policymakers must be careful to avoid reinforcing existing prejudices and inequalities, which are magnified by a broadening techno-social divide.

A. Small Data Concerns

The experimentation with, and deployment of, innovative technologies in classrooms and schools have raised fears of abuse at both the micro and macro level. At the micro, "small data" level, critics have condemned the impact of ed tech on children's learning experience. While adaptive learning and personalization promise better tailored, individualized education, they also raise concerns about privacy, fairness, and the future of education. Critics argue that such personalization turns learning into a mechanized process,

180. GOOGLE, HIPAA COMPLIANCE & DATA PROTECTION WITH GOOGLE APPS (Apr. 6, 2015), https://static.googleusercontent.com/media/www.google.com/en/US/work/apps/terms/2015/1/hipaa_implementation_guide.pdf.

with children's gazes transfixed to multiple screens and software guiding students through a series of automated choices.[181] This, in turn, removes agency, experimentation, exploration and creativity—which make human learning the fascinating process it is and distinguish it from machine learning.

1. Predictive Sorting

Data driven ed tech provides education institutions with robust tools to improve teaching and instructional methods; diagnose students' strengths and weaknesses; adjust materials and approaches for individual learners; identify at-risk students so teachers and counselors can intervene early; and more. But at the same time, these same tools can fuel the stratification of society by channeling "winners" to a "Harvard track" and "losers" to a "blue collar" track. Further, they can overly limit the right of individuals to fail, struggle, and learn through experimentation.

Consider IBM's Predictive Analytics Solution for Schools and Educational Systems (PASSES).[182] PASSES is designed to increase visibility into the performance of individual students, proactively identify at-risk students through early detection of factors affecting performance, and enable early intervention and just-in-time responses. According to the Organization for Economic Cooperation and Development, the United States, which had the world's highest rate of high school graduation in 1970, has slipped to number twenty-one in the world today,[183] with more than seven thousand students dropping out of high schools around the country *every single school day*.[184] Student failure has enormous consequences for the students themselves, as well as their families, communities, and society as a whole. On the one hand, by identifying early predictors of success or failure, IBM's PASSES helps increase graduation rates and keep students in schools. On the other hand, some fear that students could find themselves stigmatized as a result of inaccurate data, faulty

181. *See* John Warner, *We Don't Need No Adaptive Learning*, INSIDE HIGHER ED (Apr. 4, 2013, 2:36 PM), http://www.insidehighered.com/blogs/just-visiting/we-dont-need-no-adaptive-learning#ixzz2zjbEVW7P.

182. *See* IBM CORP., IBM PREDICTIVE ANALYTICS SOLUTION FOR SCHOOLS AND EDUCATIONAL SYSTEMS (2013), *available at* http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=YTS03068USEN&appname=wwwsearch.

183. *See* Stephanie Banchero, *High-School Graduation Rate Inches Up*, WALL ST. J. (Jan. 22, 2013, 12:01 AM), http://online.wsj.com/news/articles/SB10001424127887323301104578256142504828724.

184. *See* Tony Miller, U.S. Deputy Sec'y, Dep't of Educ., Remarks at the Church of God in Christ's International AIM Convention in Houston, Texas (July 7, 2011), *available at* http://www.ed.gov/news/speeches/partnering-education-reform.

algorithms, or both, or stripped of a possibility to change course, enhance their performance, and permanently absolve themselves of past failures.

2. Chilling Effect

One unfortunate upshot of predictive scoring may be defensive withdrawal of students from education systems for fear of being scored, classified, and stigmatized. Worse, such a preemptive strategy could be socially regressive, with students from wealthy families moving to private schools that operate outside of the panoptic grid. Clearly, for children who believe that every page view and quiz response will be recorded and analyzed, life under the magnifying glass becomes a grueling and relentless test. Such a trend has been predicted by authors such as David Eggers, who envisaged a dystopian society where failure to participate in the "data economy" immediately casts doubt on an individual's moral character.[185] This, in turn, could lead to a "market of lemons," where an individual's attempt to create a zone of privacy or obscurity automatically implies failure, weakness, or vice.[186] Danah Boyd and Alice Marwick have documented teens' reaction strategies to an environment of constant surveillance, including employing steganography and other means of hiding in plain sight.[187] This portends a future where students have to drop out of the system to preserve their "right to be let alone."[188]

3. Narrowcasting and Filter Bubbles

Joseph Turow has argued that increased personalization based on opaque profiling algorithms poses a risk to open society and democratic free speech.[189] He explained that, by "pigeonholing" individuals into pre-determined categories, automated decision making compartmentalizes society into pockets, or "echo chambers," of like-minded individuals. The ability to amass granular information

---

185. *See* Margaret Atwood, *When Privacy Is Theft*, N.Y. BOOKS (Nov. 21, 2013), http://www.nybooks.com/articles/archives/2013/nov/21/eggers-circle-when-privacy-is-theft/ (reviewing DAVE EGGERS, THE CIRCLE (2013)).

186. *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 48 Q. J. ECON. 488 (1970), *available at* http://socsci2.ucsd.edu/~aronatas/project/academic/Akerlof%20on%20Lemons.pdf.

187. Boyd & Marwick, *supra* note 148.

188. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

189. JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH (2011). For similar arguments, see ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011).

regarding individuals' viewing habits and target specially tailored content at them raises concerns over siloization and narrowcasting. As Joseph Turow puts it, "the industrial logic behind the[se] activities makes clear that the emerging marketplace will be far more an inciter of angst over social difference than a celebration of the 'American salad bowl.'"[190]

Such concerns already cast a shadow on the future of marketing and online content distribution, but they are far more alarming in the context of K–12 education. A child who stumbles in a quiz or test gets demoted to a lower category and thus begins a downward spiral culminating in significant, formative effects on his future path from school into the workforce. Another student is prevented from encountering information that challenges his biases or assumptions, thereby becoming more rigid and dogmatic in his approach.

Of course, these dangers, which represent inappropriate or flawed implementation, should not prevent the adoption of information technologies. Technology evangelists argue that, far from constraining a student's worldview, adaptive learning technologies have precisely the opposite effect. They enable every student to unleash his or her potential through exposure to the maximum possible enrichment that is available for them.[191] The low-tech alternative, they claim, is for students to be lumped into a class with a diverse student body—some struggling and some advanced, with teachers who, at best, scramble to satisfy the mean.

B. Big Data Concerns

The collection, assembly, and use of longitudinal records for performance measurement promise enhanced efficiencies in resource allocation and fact-based development of education policy. At the same time, they raise macro level, or "big data," fears about exposing students from a young age to a constant, panoptic gaze; subjecting disadvantaged populations to new and discreet forms of discrimination; and unleashing human subject research unbound by ethical rules. Critics say such uses of big data will stifle students' creativity, breed conformism, and upend special support structures

190. JOSEPH TUROW, NICHE ENVY: MARKETING DISCRIMINATION IN THE DIGITAL AGE 2 (2006); *see also* Andrew Leonard, *How Netflix is Turning Viewers into Puppets*, SALON (Feb. 1, 2013, 5:45 AM), http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets.

191. *See, e.g.*, David Robinson, *Are We Rushing to Judgment Against the Hidden Power of Algorithms?*, FREEDOM TO TINKER (July 30, 2014), https://freedom-to-tinker.com/blog/dgr/are-we-rushing-to-judgment-against-the-hidden-power-of-algorithms.

that schools have meticulously created to support students at risk.[192] Reformers counter that it would be unfortunate to forgo the tremendous benefits of big data based on fears of worst-case scenarios that are unlikely to materialize and can be minimized with solid data governance strategies.

1. A Surveillance Society

Evgeny Morozov cautions against surrendering the benefits of traditional, albeit imperfect, education methods to the sanitized environments of technology-mediated adaptive learning. He further cautions against a dystopian future where authoritarian governments create dashboards to monitor and control the developmental evolution of students from childhood to adulthood. He asks, "[w]ill students with low engagement scores on key events of the national history be invited to talk with the local equivalent of the KGB?"[193] Even in a free society, granular data generated by students' page views, clicks, underlinings and multiple choice answers could become part of an ominous "individual dossier," which colleges use for admission decisions, employers for hiring, and marketers for tailoring content and ads. With this in mind, Morozov argues that adaptive learning will have a chilling effect, as "the odds are that students will think twice about reading something subversive or not reading something conventional."[194] And if this is the case in the United States, with its strong constitutional protections for free speech, it will no doubt be the case in countries such as India or South Korea, which have weaker civil rights safeguards.[195]

2. Discrimination

Big data analysis can breed discrimination. As the White House recently observed, "'perfect personalization' also leaves room for subtle and not-so-subtle forms of discrimination in pricing, services,

192. Rachel Aviv, *Wrong Answer*, NEW YORKER (July 21, 2014), http://www.newyorker.com/magazine/2014/07/21/wrong-answer?currentPage; Javier C. Hernández, *Common Core, in 9-Year-Old Eyes*, N.Y. TIMES, June 14, 2014, http://www.nytimes.com/2014/06/15/education/common-core-in-9-year-old-eyes.html.

193. Evgeny Morozov, *In Soviet Russia, Book Reads You*, SLATE (Nov. 27, 2012), http://www.slate.com/articles/technology/future_tense/2012/11/coursesmart_analytics_whispercast_the_danger_of_software_that_monitors_students.html.

194. *Id.*

195. *See id.*

and opportunities."[196] Data analytics can mask discriminatory intent behind multiple masks and proxies, rendering it difficult to combat.[197] Some discriminatory criteria are clear, such as zip code-based "redlining," but others are more nuanced, muted, based on hidden correlations, and potentially unbeknown even to users. For many years, critics have argued that standardized tests were racially, socioeconomically, and gender biased.[198] Researchers have claimed, for example, that the SAT is both culturally and statistically biased against African Americans, Hispanic Americans, and Asian Americans.[199] Others maintained that reading comprehension tests do not evaluate reading comprehension skills, but rather reveal a student's pre-existing knowledge about the subject matter.

On the other hand, big data does not only *create* discrimination problems; it can also help *solve* them. The White House Report also notes, "The same big data technologies that enable discrimination can also help groups enforce their rights. Applying correlative and data mining capabilities can identify and empirically confirm instances of discrimination and characterize the harms they caused."[200] This has been the case in instances outlined above, where big data analysis surfaced persistent discrimination against African Americans in the STEM field.

3. Human Subject Research

Big data analysis unleashes human subject research unbound by ethical norms. Today, everyone—including businesses, governments, private citizens, and platform operators—has become a "researcher," analyzing the data exhaust produced by individuals' daily lives to identify useful patterns and correlations.[201] And while

196. WHITE HOUSE REPORT, *supra* note 4, at 7; *see also* Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMM. ASS'N COMPUTING MACHINERY 44 (2013), http://dataprivacylab.org/projects/onlineads/1071-1.pdf.

197. *See* Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. TELECOMM. & HIGH TECH. L. 351 (2013), *available at* http://www.jthtl.org/content/articles/V11I2/JTHTLv11i2_Polonetsky.PDF.

198. *See* Katherine Connor & Ellen J. Varyas, *The Legal Implications of Gender Bias in Standardized Testing*, 7 BERKELEY WOMEN'S L.J. 13 (1992), *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1063&context=bglj.

199. *See* Roy O. Freedle, *Correcting the SAT's Ethnic and Social-Class Bias: A Method for Reestimating SAT Scores*, 73 HARV. EDUC. REV. 1 (2003). See more recently, Maria Veronica Santelices & Mark Wilson, *Unfair Treatment? The Case of Freedle, the SAT, and the Standardization Approach to Differential Item Functioning*, 80 HARV. EDUC. REV. 106 (2010).

200. WHITE HOUSE REPORT, *supra* note 4.

201. Consider, for example, the recent outcry over Facebook's experiment with user emotions, Vindu Goel, *Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES, June 29, 2014, http://www.nytimes.com/2014/06/30/

the stakes may be limited when big data is scrutinized for the purpose of targeted ads, they weigh heavy when shaping the future of children. These ethical risks are particularly salient as the education system strengthens its partnership with the private sector.

Consider the LENA program rolled out by Providence, Rhode Island, to improve early childhood language development in poor families. Under this program, kids received "smart" clothing wired to record daily conversations. The vendor, LENA, an non-governmental organization (NGO), describes its product as "allow[ing] you to easily collect, process, and analyze language environment and development data for children ages 2 to 48 months."[202] Criticizing the adoption of the program as new "social-engineering surveillance," Christine Rosen, a fellow at the New America Foundation, wrote, "[t]he lack of concern about how state surveillance of private citizens—even in the interest of 'improving' those citizens—is increasing with little public debate about the challenges such interventions pose to freedom and autonomy."[203]

Ethical ground rules are generally needed to regulate big data based human subject research, even more so when children's data is involved.

C. A Path Forward

While stronger data governance mechanisms and trust between stakeholders can help resolve ed tech's regulatory problems, big data in the classroom will continue to provoke ethical concerns about algorithmic decision making and the role of technology in the field of education. This section suggests parents must be empowered with access to their children's data as well as enhanced transparency into algorithmic decision-making processes. This, in turn, will enable them to participate in shaping their children's educational environment.

1. Data Featurization

In previous articles, the authors have argued for a need to "featurize" data. That is, to make it a consumer-side feature not only

technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html. *But cf.* Christian Rudder, *We Experiment On Human Beings!*, OK CUPID TRENDS, (July 28, 2014), http://blog.okcupid.com/index.php/we-experiment-on-human-beings.

202. *Automatic Language Assessment in Three Easy Steps*, LENA, http://www.lenafoundation.org/customer-resources/download-center/ (last visited Apr. 17, 2015).

203. Christine Rosen, *We Need a Nuremberg Code for Big Data*, SLATE (June 20, 2013, 7:17 AM), http://www.slate.com/articles/technology/future_tense/2013/06/providence_talks_program_and_the_rise_of_social_engineering_surveillance.html.

collected from individuals and harnessed by business but also made readily available for individuals to use. This same concept is key in the education sphere. Parents need to experience the *value* of data in order to buy into the ed tech revolution. Data featurization includes dashboards for parents, not just school officials, providing 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, hungry for more. Parents should benefit from access to data before the end of a quarter and 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. And while FERPA already requires parent access, this right is only 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 third-party apps and tools.

The featurization idea is already reflected by 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,[204] a digital backpack can provide parents with confidence that data is not only used to assess and rate their children's performance but also utilized 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 parents' privacy concerns.[205]

2. Algorithm Transparency

In *Big Data For All: Privacy And User Control In The Age Of Analytics*,[206] the authors previously explained that in a world of big data, transparency must extend beyond simple access to raw information in order to provide individuals with insight into the inner working of the machine. The article stated, "To minimize concerns of untoward data usage, organizations should disclose the logic

204. WHITE HOUSE REPORT, *supra* note 4, at 14.

205. SIIA's Vision K20 finds that education's implementation of e-portfolios ranks last on a list of twenty ways that schools can more effectively use technology at just 1.35 on a scale of 1–4. *See* SOFTWARE & INFO. INDUSTRY ASS'N, VISION K–20 SURVEY RESULTS (June 2014), *available at* http://www.siia.net/visionk20/2014_VK20.pdf.

206. 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.

underlying their decision-making processes to the extent possible without compromising their trade secrets or intellectual property rights."[207] The article explained that individuals must understand the decisional criteria of organizations "lest they face a Kafkaesque machinery that manipulates lives based on opaque justifications."[208]

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."[209] 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."[210] 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.

3. 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 inequality. Unfortunately, broad disparities persist in the performance of African American and Hispanic students compared to their white peers. 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.

Privacy advocates should be cautious of advocating reforms that might undermine the operation of such institutions. 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

207. *Id.* at 243.

208. *Id.*

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

210. *Id.*

the required opt-in forms, those students may miss out on valuable education opportunities. Meanwhile, private and charter schools, which are relatively free of regulatory obligations, will continue to aggressively pursue ed tech and data solutions to advance student performance. In the marketing context, policymakers pay little heed to whether users opt-in or opt-out of ad delivery platforms. But in the education area, opting out may be akin to dropping out.

It is also important to recognize that schools no longer account for the entirety of a student's educational experience. Families, including in high-poverty and minority groups, are supplementing school activities with apps, tutoring centers, after-school clubs, and informal learning opportunities. The robust information assembled about a student in school can be leveraged outside of school to create a more seamless and customized learning process. Locking down data in school coffers for fear that vendors will inappropriately use it for marketing could undermine opportunities to empower families with the information and recommended appropriate learning modules.

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.[211]

VI. 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. For too long, education has been data rich and information poor, collecting massive amounts of data but keeping it in formats and silos that hindered access and usability.

At the same time, data driven ed tech presents new risks to student privacy; raises ethical concerns about unfairness and discrimination; and threatens to upend the delicate balance between stakeholders involved in public education, including federal and state

211. *See* Brenda Leong & Jules Polonetsky, *Why Opting Out of Student Data Collection Isn't the Solution*, EDSURGE (Mar. 16, 2015), https://www.edsurge.com/n/2015-03-16-why-opting-out-of-student-data-collection-isn-t-the-solution.

governments, school districts, schools, teachers, and parents, as well as businesses, academic leaders, and think tanks. Consequently, the arrival of ed tech has been rife with controversy, too often conflating issues such as student privacy and parental rights with policy debates around standardization and the role of government in K–12 education.

While there is a long history of commercial activities within schools and commercial use of student data in this country, the legal framework designed to protect students' privacy is now outdated and laden with gaps. Parents, schools, students, and vendors seeking to make the most out of student data must first navigate the complex patchwork of state laws, prone to reactionary short-sightedness; agency regulations, filled with ambiguity; and federal legislation, unclear in scope and unfit for modern business and technological realities. There is a shortage of trust between all stakeholders, impeding ed tech from realizing its tremendous promise of better, more accessible education for all.

It is critical that stakeholders move quickly to address real shortcomings in school privacy, starting by ensuring that schools have the capacity for data governance, training of essential personnel, and basic auditing skills. Gaps in FERPA and COPPA must be filled to better adapt the legislation to current technological realities. These responses can proceed in a well-tread path charted by multiple policy initiatives, including reform of US and international privacy legislation and an emerging body of FTC enforcement actions.

More broadly, policymakers must ensure additional data transparency to engender trust, tapping into both traditional forums such as town hall meetings and innovative solutions such as digital backpacks, data featurization, and algorithm transparency. Without measures to help parents understand how data are used to help their children's progression, the debate about data in education will remain polarized. With them, ed tech will be further harnessed to democratize education, tailor solutions for individual student needs, and provide objective metrics for measurement and accountability.