STUDENT PRIVACY PRINCIPLES FOR THE AGE OF BIG DATA: MOVING BEYOND FERPA AND FIPPS†

*Elana Zeide**

ABSTRACT

The literature on student privacy often focuses on specific provisions and definitions. This Article offers a broader perspective on how the regulatory mechanisms of FERPA and new reforms work within today's technological, institutional, and economic systems. It makes several contributions, including (1) analyzing the assumptions that underlie FERPA's FIPPs-based approach to privacy; (2) finding such protections insufficient in light of the technological and information infrastructure created by networked systems, cloud computing, and big data analytics that are often provided by private entities; and (3) enumerating practical, political, pedagogical, and philosophical characteristics of America's education system that limit the efficacy of privacy protection through personal or institutional self-management.

FERPA nominally operates on the notion of notice and consent but in practice delegates the bulk of data-related decisionmaking to educators through the school official exception. The statute defers to educators' unspecified and undocumented criteria for disclosure. It imposes no direct accountability for violations given the "nuclear" nature of enforcement through withdrawal of federal funding.

FERPA's reliance on institutional approval and access and amendment rights offered stakeholders sufficient reassurance given the limitations of physical records that were not readily accessible, portable, or incorporated into daily institutional practice. Today, educators cannot cope with the

---

† This Article has been updated to correct a formatting error in the original abstract. The Article should now be cited as "Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339 (2016) (online corrected)."

* Fellow, Information Law Institute, New York University School of Law and Affiliate, Data & Society Research Center. I am grateful for the invaluable advice of my colleagues and NYU's Privacy Research Group, especially Seda Guerses, Joris Van Hoboken, Karen Levy, Nathan Newman, Helen Nissenbaum, Ira Rubenstein, Katherine Strandburg, and Malte Zweitz. Thank you to Kwaku Awokuah, Michael Burstein, danah boyd [sic], Monica Bulger, Kate Crawford, Sue Glueck, Michael Hawes, Joseph Jerome, Brenda Leong, Mark Luetzelschwab, Mark MacCarthy, Steve Mutkowski, Leonard Niehoff, Jules Polonetsky, Joel Reidenberg, Dalia Topelson Ritvo, Jason Schultz, Daniel Solove, Mitchell Stevens, Kathleen Styles, and Amelia Vance for your generous contributions and support.

burden of tracking and policing recipients' information practices given the proliferation and complexities of today's data-driven infrastructures. The resulting system places untenable burdens on students, parents, and educators that often fails to provide either actual oversight over disclosed information or meaningful transparency, accountability, and scrutiny over schools' information practices.

Context-specific characteristics also make reliance on FIPPs-based privacy protection practically problematic and theoretically unsound. Opting out by withholding consent is rarely a realistic option given the compulsory nature of primary and secondary education and the competitive pressure on students to obtain credentials from higher education institutions to ensure future opportunities. On a practical level, considering individual privacy preferences would overwhelm educators and administrators. Politically, FERPA's delegation model accommodates the decentralized political authority and extreme heterogeneity of American's locally-governed education system. Pedagogically, privacy self-management may have problematic effects as changing information practices changes the content, methodology, and measurement of instruction. Philosophically, shifts in data flow change the content, goals, and values of education itself in fundamental ways. These realities must inform future policymaking rather than reliance on a regulatory model poorly designed for today's educational ecosystem.

TABLE OF CONTENTS

OVERVIEW

This Article demonstrates that FERPA's regulatory regime does not address contemporary student privacy[1] concerns raised by the rise of big data analytics and data mining. The statute regulates the disclosure of student information by schools to outside entities on a model that, theoretically, provides parents and students with control over information. In practice, however, FERPA delegates decision-making authority to schools without requiring meaningful oversight, transparency, or accountability regarding specific data practices.

Part I describes new information practices prompted by technological innovation and the rise of data-driven education management, pedagogy, and policymaking. Interactive digital platforms automatically collect more detailed information about students from a variety of sources, including social media and physical facilities and operations. Cloud computing bridges previously incompatible data silos. At the same time, it increases the risk of unauthorized access to student information, allows for unintentional and unknowing disclosure, and frequently entails data recipients generating and storing student information themselves beyond school control. The rise of big data analytics creates new ways to use information to enhance students' education and learn more about learning itself. In addition, it creates institutional and financial incentives to put student information to secondary uses serving both educational and non-educational purposes.

Part II details and analyzes FERPA's regulatory scheme. The statute's privacy protection provision focuses on ensuring that schools only disclose personally identifiable student information with parents' consent or educators' approval. Despite default provisions based on the Fair Information Practices Principles (FIPPs), FERPA actually delegates most decision-making of student privacy to educational institutions and entities, without requiring meaningful transparency, oversight, or direct accountability.[2] Numerous exceptions to the statute's consent requirement—particularly the "School

1. This Article focuses on student data collected in traditional, publicly funded educational institutions that fall under FERPA's purview. Education data also impacts other actors in the system including teachers, schools, districts, and local and state education agencies, their employees, and alumni, but consideration of the broader impacts on education privacy is beyond the scope of this Article.

2. *See infra* Part II.B.

Official Exception" that allows schools to share information with online providers—give educational actors broad discretion while requiring minimal documentation and transparency.[3] Schools and districts have broad discretion to determine whether sharing student data with a particular recipient serves a legitimate educational interest and what measures are required to ensure data recipients use student information appropriately and securely.[4]

Part III examines how new information practices have upset the underlying principles that made FERPA's student privacy protections acceptable for almost forty years. FERPA's efficacy rested on assumptions about information practices that no longer hold true given today's technological capabilities. The limited portability, permeability, and ability to repurpose paper records restricting disclosure to approved recipients prevented unauthorized actors from accessing student information and, in doing so, presumably limited inappropriate use or repurposing. Today, FERPA's reliance on educational actors' approval of data recipients does not account for unauthorized, accidental, and frequently unknowing disclosure of personally identifiable student information to outside parties.[5] For example, teachers may create de facto school official relationships simply by accepting click-wrap terms of service.[6]

FERPA's delegation-based regulatory framework is an ineffective tool for imposing specific constraints and for creating liability and accountability. Additionally, the statute's current compliance-orientation also permits a fair degree of accidental, unavoidable, or unknowing noncompliance without imposing any consequences.

Part IV analyzes the FERPA amendments proposed to address these concerns. These bills add procedural requirements, increased transparency, and more opportunities for parents and students to exercise consent.[7] The amendments also impose substantive restrictions on certain information practices of educational actors[8] and create direct accountability for educational actors through the crea-

3. *See* 34 C.F.R. § 99.31(a)(1)(i)(B) (2014).

4. *See* CONSORTIUM FOR SCHOOL NETWORKING, PROTECTING PRIVACY IN CONNECTED LEARNING TOOLKIT 19 (2014) [hereinafter COSN], *available at* http://www.cosn.org/sites/default/files/Privacy%20Toolkit_0319.pdf.

5. *See id.*

6. *See* COSN, *supra* note 8, at 18 (discussing that if the provider will be using FERPA-protected information, schools and districts should exercise caution when entering into click-wrap agreements that allow for amendment without notice, given FERPA's requirement to maintain "direct control" over the use and maintenance of the information under the School Official Exception).

7. *See infra* Part IV.

8. *See* COSN, *supra* note 8, at 15–17.

tion of a private right of action and fines for noncompliance.[9] Finally, they also regulate data recipients indirectly by creating additional qualifications and requiring contractual stipulations.[10]

Part V discusses additional reforms necessary to address the upset of information norms that made FERPA's delegation model framework acceptable for almost forty years. These reforms include increasing transparency of information practices regarding student information, imposing procedural and governance requirements to provide more documentation of data flow, and requiring schools to have a comprehensive inventory of their information ecosystem, in a strong effort to regulate educational actors' collection, use, storage, and retention of student information.

Many of the proposed changes cannot provide the control over personal data and the reassurance sought by stakeholders because these bills still rely on FIPPs-based privacy protection within FERPA's delegation-oriented regulatory structure and do not consider the distinct characteristics of the education context.[11] FIPPs-based privacy protection is both ineffective and theoretically unsound in the education context. Notions of notice and consent are particularly problematic in the education context where student participation is compulsory, or frequently coerced. FERPA's delegation model also accommodates the need for institutional, rather than individual, decision-making in education. Privacy self-management also poses practical, pedagogical, political, and philosophical difficulties distinct to the education context.

Further, regulating non-educational actors indirectly through FERPA's framework is untenable. Whether reforms create more conditions for data recipients or require certain written stipulations before disclosure, they still place the burden of investigation, oversight, and potential liability on educational actors. Education institutions simply do not have the infrastructure or resources to evaluate and monitor third-party information practices.

Instead of imposing more requirements on data recipients or relying on stipulated clauses in private rulemaking between the parties, policymakers should regulate worrisome actors and practices directly. This is not only more effective, but will provide clear regulation that simplifies matters for educational actors and data recipients and reassures stakeholders that student privacy is soundly protected.

---

9. *See infra* Part IV.B.

10. *See* CoSN, *supra* note 8, at 15–17.

11. *See infra* Part IV.C.

At the same time, accountability mechanisms in education must allow for the heterogeneity of the education system. It must take into account the ultimate goals of the education context to serve students and to understand that fines or private rights of action may deplete schools' scant resources and, in doing so, hurt the students the regulations seek to protect.

Consequently, FIPPs-based individual control over information and FERPA's delegation of decision-making is insufficient to provide adequate student privacy protection. Rather than refining a regulatory model not designed to provide the control and oversight sought in today's educational ecosystem, policymakers should focus on reforms that ensure baseline protection of student information, regulate problematic actors and practices directly, and create appropriate consequences for misuse and mismanagement.

I. THE CURRENT STUDENT PRIVACY LANDSCAPE

Education is increasingly data-reliant and data-driven.[12] Fundamental shifts in what information is collected, who it is shared with, how it is used, how long it is stored, and what uses it can be put toward have unsettled entrenched expectations about information flow in education. The low cost storage, transfer, and improved analytic capabilities available through cloud computing,[13] the push for data-driven education,[14] and the rise of industries based on monetizing data have prompted key changes in the attributes, recipient, and transmission principles governing the flow of student information.[15]

A. Data-Driven Education: New Applications and Recipients

Digital tools collect more detailed information about students, including data created during the course of instruction with interactive applications, from a variety of sources, including social media and physical facilities and operations. Cloud computing not only bridges previously incompatible data silos, but also increases the potential for unauthorized access to student information, allows for

12. *See, e.g.*, Allie Gross, *A Brief History of Education's Big Data Debate*, EDUCATION DIVE (May 7, 2014), http://www.educationdive.com/news/a-brief-history-of-educations-big-data-debate/258602/.

13. Kingsley Osei, *Pouring New Wine into Old Wineskins: Why "On Premise" Software Source Code Escrow Arrangements Are Ill-Suited for Remotely Hosted "Off Premise" Software as a Service License Agreements*, 39 J.C. & U.L. 383, 384–85 (2013).

14. *See* Audrey Watters, *Student Data Is the New Oil: MOOCs, Metaphor, and Money*, HACK EDUC. (Oct. 17, 2013), http://hackeducation.com/2013/10/17/student-data-is-the-new-oil.

15. *See generally* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

unintentional and unknowing disclosure, and frequently entails data recipients generating and storing student information themselves. Finally, the rise of big data analytics creates new ways to use information to enhance students' education and learn more about learning itself. It also allows and creates institutional and financial incentives to put student information to secondary uses serving both educational and non-educational purposes.

Educational institutions frequently outsource information management and data-reliant services to third-party specialists.[16] Both lower and higher education institutions increasingly share information with a broad array of specialized service providers who facilitate administration, communication, instruction, assessment, and operational functions—as well as the creation of Statewide Longitudinal Data Systems—and require reporting to state educational agencies and the U.S. Department of Education (DOE).[17]

These data recipients may provide document management, email and messaging, or search engines (Microsoft, Google).[18] They offer tools designed to help education institutions manage student information (SIS), and provide interoperable data repositories (Learning Registry, the ill-fated inBloom).[19] They may also offer learning management systems that consolidate the administration, documentation, tracking, reporting, and delivery of electronic educational technology[20] (Google Classroom, Blackboard, Naviance).[21]

---

16. *See generally* U.S. Dep't of Educ. Privacy Technical Assistance Ctr., *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (Feb. 2014), *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf; José A. González-Martínez et al., *Cloud Computing and Education: A State-of-the-Art Survey*, 80 COMPUTERS & EDUC. 132 (2015); LARRY JOHNSON ET AL., NMC: HORIZON REPORT: 2014 HIGHER EDUCATION EDITION (2014), *available at* http://www.nmc.org/pdf/2014-nmc-horizon-report-he-EN.pdf.

17. *See, e.g.*, Jules Polonetsky & Omer Tene, *Who Is Reading Whom Now: Privacy in Education from Books to MOOCs*, 17 VAND. J. ENT. & TECH. L. 927, 938 (2015) [hereinafter Polonetsky & Tene, *Who Is*]; Leah Plunkett, Alicia Solow-Niederman & Urs Gasser, *Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014*, BERKMAN CTR. FOR INTERNET & SOC'Y (June 3, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2442432; U.S. Dep't of Educ. Inst. of Educ. Scis., *Statewide Longitudinal Data Systems Grant Program – Program Overview*, NAT'L CTR. FOR EDUC. STATS., http://nces.ed.gov/Programs/SLDS/index.asp (last visited May 25, 2016).

18. *See* Plunkett, Solow-Niederman & Gasser, *supra* note 21, at 6.

19. *Id.;* LEARNING REGISTRY, http://learningregistry.org/ (last visited May 10, 2016); Natasha Singer, *InBloom Student Data Repository to Close*, N.Y. TIMES (April 21, 2014), http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/.

20. *See* Polonetsky & Tene, *Who Is*, *supra* note 21, at 934–40.

21. GOOGLE CLASSROOM, https://support.google.com/edu/classroom/answer/6020279?hl=en (last visited Apr. 18, 2016); BLACKBOARD, http://www.blackboard.com (last visited Apr. 18, 2016); NAVIANCE, http://www.naviance.com (last visited Apr. 18, 2016).

Student information drives digital instructional material like e-textbooks (MyON, TumbleBooks), learning games (Duolingo), online tutoring (Khan Academy), and entire course platforms (edX, Coursera).[22] Data recipients may provide digital and adaptive coursework and assessment, along with detailed reports for students and teachers (McGraw-Hill's Learn Smart, Pearson's MyLab & Mastering with Adaptive Learning, Smarter Balanced Assessment Consortium).[23] They can assess and track classroom behavior (ClassDojo).[24] They may monitor student work for plagiarism (Turnitin).[25] Student data is shared through online applications to colleges for financial aid or digital transfer and submission of transcripts and credentials (Parchment).[26]

Schools[27] also share information with outside parties providing administrative services like eBilling (Empower), emergency notification (School Messenger), community outreach (BoardDocs), and polling (SurveyMonkey).[28] These outside parties provide services designed to facilitate the use of diverse digital services through centralized ("federated") identification management (Clever).[29] Schools

22. *See* Polonetsky & Tene, *Who Is*, *supra* note 21, at 936–37; MYON, https://www.myon.com (last visited Apr. 18, 2016); TUMBLEBOOKS, https://www.tumblebooks.com (last visited Apr. 18, 2016); DUOLINGO, https://en.duolingo.com (last visited Apr. 18, 2016); KHANACADEMY, https://www.khanacademy.org (last visited Apr. 18, 2016); EDX, https://www.edx.org (last visited Apr. 18, 2016); COURSERA, https://www.coursera.org (last visited Apr. 18, 2016).

23. *See* Polonetsky & Tene, *Who Is, supra* note 21, at 939; *Help Students Learn Faster, Study More Efficiently, and Retain More Knowledge*, MCGRAW HILL EDUC., http://www.mheducation.com/prek-12/platforms/learnsmart.html; *MyLab & Mastering*, PEARSON, http://www.pearsonmylabandmastering.com (last visited Apr. 18, 2016); SMARTER BALANCED ASSESSMENT CONSORTIUM, http://www.smarterbalanced.org (last visited Apr. 18, 2016)

24. Polonetsky & Tene, *Who Is, supra* note 21, at 952, 975; CLASSDOJO, https://www.classdojo.com (last visited Apr. 18, 2016).

25. TURNITIN, http://turnitin.com (last visited Apr. 18, 2016).

26. PARCHMENT, http://www.parchment.com (last visited Apr. 18, 2016); *see also CourseTalk Partners with Parchment to Expand College Opportunities for Students*, BUS. WIRE (Apr. 29, 2014), http://www.businesswire.com/news/home/20140429005809/en.

27. Under FERPA, the same provisions apply to schools, districts, and local educational agencies as "educational institutions." For the sake of brevity, I only refer to "schools" over the course of this Article. The phrase "education institutions" also has specific meaning with respect for FERPA, but for the purposes of this Article I use it to refer broadly to schools that may or may not fall under the statutes' purview.

28. *See Billing and Receivables*, EMPOWER STUDENT INFO. SYS., https://www.empowersis.com/features/billing-receivables (last visited Apr. 18, 2016); SCHOOLMESSENGER, http://www.schoolmessenger.com/ (last visited Apr. 18, 2016); *Education, School, and Academic Online Surveys*, SURVEYMONKEY, https://www.surveymonkey.com/mp/education-surveys (last visited Apr. 18, 2016).

29. *See* CLEVER, https://clever.com (last visited Apr. 18, 2016); *see also* Patrick Hoge, *Clever Raises $30 Million as Schools Nationwide Adopt Its Software Management Tools*, S.F. BUS. TIMES (Dec. 16, 2014, 5:00 AM), http://www.bizjournals.com/sanfrancisco/blog/2014/12/clever-funding-education-schools-software.html.

also share information while outsourcing operational functions like eCommerce (MySchoolBucks), transportation (TripDirect), and security (Radiant RFID).[30]

At a classroom level, educators frequently adopt cloud-based applications to assist with course management, grading, and instruction; in particular, social networking tools (Facebook, Twitter, Edmodo).[31] While some districts have adopted policies governing the use of new technology, and a few have created lists of vetted applications, some districts provide teachers with minimal guidance and oversight.[32] In many cases, teachers do not have to report their use of free or "freemium" tools, or receive approval to use those tools.[33]

B. Digital Data Collection: Expanded Attributes and Sources

Digital, data-driven, and interactive educational tools and platforms generate more granular information about students than has previously been possible.[34] This includes not only consciously disclosed or entered information, but also metadata that contains information about students' keystrokes, mouse movements, and time/location stamps.[35] Student ID cards may collect location data when students access school facilities and financial information if

30. MYSCHOOLBUCKS, https://www.myschoolbucks.com (last visited Apr. 18, 2016); FS DIRECT, https://www.schooldude.com/solutions/products/TripDirect (last visited Apr. 18, 2016); *RFID Mustering Solutions*, RADIANT RFID, http://www.radiantrfid.com/education-mustering.html (last visited Apr. 18, 2016).

31. Tahnja Wilson, *Using Twitter and Facebook to Encourage Student Classroom and Political Engagement*, TEACHONLINE (Feb. 6, 2015), https://teachonline.asu.edu/2015/02/using-twitter-facebook-encourage-student-classroom-political-engagement; *see also* Plunkett, Solow-Niederman, & Gasser, *supra* note 21, at 2; EDMODO, https://www.edmodo.com (last visited Apr. 18, 2016).

32. *See* JOEL R. REIDENBERG ET AL., PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 24 (2013), *available at* http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip [hereinafter CLIP STUDY].

33. *Teacher Apps Raise Student Privacy Concerns*, CONNECT LEARNING TODAY (Mar. 25, 2015), http://connectlearningtoday.com/teacher-apps-raise-student-privacy-concerns.

34. *See* OFFICE OF EDUC. TECH., U.S. DEP'T OF EDUC., ENHANCING TEACHING AND LEARNING THROUGH EDUCATIONAL DATA MINING AND LEARNING ANALYTICS: AN ISSUE BRIEF 1, 9 (2012), *available at* https://tech.ed.gov/wp-content/uploads/2014/03/edm-la-brief.pdf; Ryan Baker & George Siemens, *Educational Data Mining and Learning Analytics*, *in* CAMBRIDGE HANDBOOK OF THE LEARNING SCIENCES 253, 253 (Keith Sawyer ed., 2d ed. 2014). For example, the inBloom database accounted for approximately 400 data points derived from the National Education Data Model (NEDM), a conceptual model of the data points educational entities might consider collecting. Singer, *supra* note 23; *see also* NAT'L CTR. FOR EDUC. STATS., http://nces.ed.gov/forum/datamodel (last visited Apr. 18, 2016).

35. *See* Polonetsky & Tene, *Who Is*, *supra* note 21, at 965; *see also* Jules Polonetsky & Omer Tene, *The Ethics of Student Privacy: Building Trust for Ed Tech*, 21 INT'L REV. INFO. ETHICS 25, 29 (2014).

used to pay for cafeteria and bookstore purchases.[36] Schools and universities may also collect information about students from non-educational sources, like social media, in order to monitor bullying, identify at-risk students, or connect like-minded classmates.[37]

C. Cloud Computing: Portability and Permeability

Schools at the primary, secondary, and post-secondary levels and districts ("education institutions") generate and oversee the growing volume of student information in the education context.[38] In doing so, they routinely rely on, and share, student data with outside entities that provide administrative, academic, information management, and operational services.[39] Disclosure of personally identifiable student information is no longer an occasional occurrence but a routine part of day-to-day school information practices.

---

36. For example, educators might use sensors to track students' eye movement while reading to detect possible learning disabilities, facilitate access to school buildings with school ID cards, or identify students with face or palm scans. *See* Polonetsky & Tene, *Who Is*, *supra* note 21, at 935 n.10.

37. *See, e.g.*, Hunter Schwarz, *Schools Can Require Students to Hand over Their Social Media Passwords Under Illinois Law*, WASH. POST (Jan. 22, 2015), http://www.washingtonpost.com/blogs/govbeat/wp/2015/01/22/schools-can-require-students-to-hand-over-their-social-media-passwords-under-illinois-law/; Jason E. Lane & B. Alex Finsel, *Fostering Smarter Colleges and Universities: Data, Big Data, and Analytics*, *in* BUILDING A SMARTER UNIVERSITY: BIG DATA, INNOVATION, AND ANALYTICS 3, 9 (Jason E. Lane ed., 2014) (discussing university mining of students' social network data).

38. *See* ISAAC MEISTER & ALICIA SOLOW-NIEDERMAN, *K-12 Edtech Cloud Service Inventory 2* (HARVARD UNIVERSITY, Berkman Ctr. for Internet & Soc'y, Research Paper No. 2014-2) , *available at* http://cyber.law.harvard.edu/node/8717; *see generally* CLIP STUDY, *supra* note 36; Baker & Siemens, *supra* note 38, at 253.

39. EMMETT MCGROARTY ET AL., COGS IN THE MACHINE: BIG DATA, COMMON CORE AND NATIONAL TESTING 3 (2014), *available at* http://www.stopccssinnys.com/uploads/Cogs_in_the_Machine.pdf; ALEX MOLNAR ET AL., SCHOOLHOUSE COMMERCIALISM LEAVES POLICYMAKERS BEHIND 1–2 (2014), *available at* http://nepc.colorado.edu/files/trends-2013.pdf; Debbie Kelley, *Colorado Parents Worry About What Government, Businesses Know About Their Kids*, COLO. SPRINGS GAZETTE (Feb. 24, 2015, 10:50 AM), http://gazette.com/colorado-parents-worry-about-what-government-businesses-know-about-their-kids/article/1546681; Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 15, 2014, 5:05 AM), http://www.politico.com/story/2014/05/data-mining-your-children-106676 [hereinafter Simon, *Big Biz*]; Stephanie Simon, *For Sale: Student "Hopes and Dreams*," POLITICO (May 15, 2014, 5:06 AM), http://www.politico.com/story/2014/05/student-data-privacy-market-106692.html [hereinafter Simon, *For Sale*]; *see* 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; Quinten Plummer, *Apps Still Tracking Kids Despite Privacy Laws,* TECH TIMES (Dec. 8, 2014, 11:38 P.M.), http://www.techtimes.com/articles/21766/20141208/apps-still-tracking-kids-despite-privacy-laws.htm; Press Release, *National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared*, COMMON SENSE MEDIA (Jan. 22, 2014), *available at* https://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern [hereinafter *Common Sense Media*].

Cloud-based applications have become the norm.[40] These platforms make data more portable and permeable than paper records, which had to be physically transferred or dictated to data recipients. Even digitized content was difficult to share until recently because accessing it typically required specialized software.[41] The ease of cloud-based applications and platforms creates tremendous utility, but also makes stored student information more subject to unauthorized access by hackers or unintentional disclosure due to human accidents or technological errors.[42] Because collection and disclosure can occur so seamlessly, educational actors may share student data unknowingly as platforms and applications automatically collect content and metadata.[43]

D. Big Data: Infinite Utility and Repurposablity

Unlike the previous systems used to handle student information, which were relegated to paper and digitized using incompatible data systems, today's student records are "datafied"—recorded, stored, and organized in a format that is portable, searchable, and computationally manipulable.[44] In addition to providing immediate services and functions, this "datafied" system enables data to be put toward secondary purposes, most notably through "big data" analyses whereby data is aggregated with other information to discover relationships between variables.[45]

---

40. *See* Claudia Diaz, Omer Tene & Seda Guerses, *The Second Wave of Global Privacy Protection: Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923, 935 (2013).

41. Darrell M. West, *Big Data for Education: Data Mining, Data Analytics, and Web Dashboards*, GOVERNANCE STUDIES AT BROOKINGS 1, 9 (2012); s*ee also* Katie Ash, *Fragmented Data Systems a Barrier to Better Schools, Experts Say*, EDUC. WEEK, (Mar 11, 2013), *available at* http://www.edweek.org/ew/articles/2013/03/14/25datadelivery.h32.html.

42. Polonetsky & Tene, *Who Is, supra* note 21 at 24-25; National School Boards Association, *Data in the Cloud: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era* (Apr. 2014), http://edu.safegov.org/media/2014-04-NSBA-Data-in-the-Cloud-Legal-and-Policy-Guide.pdf; *see generally* Bill Fitzgerald, *The Day and the Data: Catching Policy Up to Reality*, FUNNYMONKEY (Jan. 30, 2014), https://funnymonkey.com/2014/the-day-and-the-data-catching-policy-up-to-reality.

43. Natasha Singer, *Privacy Pitfalls as Education Apps Spread Haphazardly*, N.Y. TIMES (Mar. 11, 2015), http://www.nytimes.com/2015/03/12/technology/learning-apps-outstrip-school-oversight-and-student-privacy-is-among-the-risks.html?_r=0.

44. Katherine J. Strandburg, *Monitoring, Datafication and Consent: Legal Approaches to Privacy in a Big Data Context*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 5, 10–12 (Julia Lane et al. eds., 2014) ("[T]he recording, aggregation, and organization of information into a form that can be used for data mining, here dubbed 'datafication', has distinct privacy implications that often go unrecognized by current law.").

45. JOHNSON ET AL., *supra* note 20, at 4.

Student data can now be analyzed and aggregated to inform instruction, chart student competencies, and predict outcomes (Panorama Education, Civitas).[46] Student data now creates profiles used by "personalized" learning platforms (Dream Box, Knewton), systems to monitor at-risk students (Purdue Course Signals, Arizona State University), and academic and career guidance (eAdvisor, Austin Peay State University).[47] These tools can generate new information about students by analyzing cumulative data or aggregating traditional academic information about student performance and enrollment, with an infinite array of variables.[48] For example, these tools can measure the likelihood of a particular student passing a course or accepting an offer from a specific college.[49]

Information collected by vendors in the course of providing services to schools can also help institutions and service providers optimize existing products and predict marketplace needs.[50] Policymakers and stakeholders increasingly use this data to evaluate educators, institutions, instructional design, pedagogical methodology, curricula, and technological applications.[51] Student information can also feed targeted marketing and advertising programs, be sold di-

---

46. Tony Wan, *Panorama Education Scores $12M to Boost Student Voice, School Success*, EDSURGE (Aug. 4, 2015), https://www.edsurge.com/news/2015-08-04-panorama-education-scores-12m-to-boost-student-voice-school-success; Eric Westervelt, *Higher Ed's Moneyball?*, NPR (Oct. 14, 2015, 4:07 P.M.), http://www.npr.org/sections/ed/2015/10/14/440886037/higher-eds-moneyball.

47. *See Knewton Brings Adaptive and Personalized Learning to the Masses*, GETTING SMART (Sept. 2, 2015), http://gettingsmart.com/2015/09/knewton-brings-adaptive-and-personalized-learning-to-the-masses/; Roger Riddell, *Adaptive Learning: The Best Approaches We've Seen so Far,* EDUCATION DIVE (Oct. 31, 2013), http://www.educationdive.com/news/adaptive-learning-the-best-approaches-weve-seen-so-far/187875/; Kimberly E. Arnold & Matthew D. Pistilli, *Course Signals at Purdue: Using Learning Analytics to Increase Student Success*, presented at Proceedings of the 2nd International Conference on Learning Analytics and Knowledge (2012); Elizabeth D. Phillips, *Improving Advising Using Technology and Data Analytics,* CHANGE: MAGAZINE OF HIGHER LEARNING (Jan.–Feb. 2013), *available at* http://www.changemag.org/Archives/BackIssues/2013/January-Februar/improving-advising-full.html; Marc Parry, *Big Data on Campus*, N.Y. TIMES (July 18, 2012), http://www.nytimes.com/2012/07/22/education/edlife/colleges-awakening-to-the-opportunities-of-data-mining.html.

48. *See* Parry, *supra* note 51*;* Polonetsky & Tene, *Who Is*, *supra* note 21, at 934–41.

49. *See, e.g.*, Rebecca Barber & Mike Sharkey, *Course Correction: Using Analytics to Predict Course Success*, *available at* http://bluecanarydata.com/wp-content/uploads/2013/05/BarberSharkey-LAKShort.pdf; Sarah Coen, *How Campuses Can Use Predictive Analytics to Focus College Student Recruitment More Strategically,* RUFFALONL (Mar. 1, 2012), http://blogem.ruffalonl.com/2012/03/01/campuses-predictive-analytics-focus-college-student-recruitment-strategically/.

50. *See, e.g.*, Polonetsky & Tene, *Who Is*, *supra* note 21, at 950–52.

51. *See, e.g.*, Gail Dutton, *Big Data Goes to School*, FORBES (Mar. 6, 2014, 5:33 PM), http://www.forbes.com/sites/emc/2014/03/06/big-data-goes-to-school/; Lisa Fleisher, *Big Data Enters the Classroom*, WALL ST. J. (Mar. 23, 2014, 4:35 PM), http://www.wsj.com/articles/SB10001424052702304756104579451241225610478.

rectly to data-driven enterprises like data brokers, or be accumulated as corporate assets.[52]

E. Contemporary Concerns

The routine incorporation of private third parties into the education information ecosystem, the use of cloud-based and permeable networks, and the repurposing potential of education-generated student information all upset the traditional information flow in the education context.[53] These changes prompt stakeholder concerns about data security, mismanagement, and misuse by educational institutions and outside parties.[54]

Some stakeholders object to the expanded collection of student information[55] and ubiquitous tracking, finding that an intrusive magnitude of harm may result from improper disclosure, misuse, or mismanagement.[56] The portability of data and the permeability of cloud-based data systems create new concerns about unauthorized

52. *See, e.g.*, Diane Ravitch, *Bill Gates' Utopian Vision for Your Child*, DIANE RAVITCH'S BLOG (Nov. 11, 2013), http://dianeravitch.net/2013/11/06/bill-gates-utopian-vision-for-your-child/; MOLNAR ET AL., *supra* note 43, at 28–29.

53. *See generally* Mark MacCarthy, *Student Privacy: Harm and Context*, 21 INT'L REV. OF INFO. ETHICS 11 (2014); *see also* Sonja Trainor, *Student Data Privacy is Cloudy Today, Clearer Tomorrow*, 96 PHI DELTA KAPPAN 13, 14 (2015), *available at* http://pdk.sagepub.com/content/96/5/13 (providing chronology of data privacy backlash).

54. *See, e.g.*, Benjamin Herold, *Americans Worried, Uninformed About Student Data Privacy, Survey Finds*, EDUC. WEEK (Jan. 22, 2014, 12:47 AM), http://blogs.edweek.org/edweek/DigitalEducation/2014/01/american_worried_uninformed_student_data_privacy.html [hereinafter Herold, *Americans Worried*]; Michelle R. Davis & Sean Cavanagh, *Cloud Computing in K-12 Expands, Raising Data Privacy Concerns*, EDUC. WEEK (Jan 7, 2014), http://www.edweek.org/ew/articles/2014/01/08/15cloud_ep.h33.html?qs=privacy; Tanya Roscorla, *Congress Urged to Update Student Data Privacy Law*, CTR. FOR DIGITAL EDUC. (June 27, 2014), http://www.centerdigitaled.com/news/congress-urged-to-update-student-data-privacy-law.html; Khaliah Barnes, *Student Data Collection Is Out of Control*, N.Y. TIMES (Dec. 19, 2014, 12:33 PM), http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data-collection-is-out-of-control; *Common Sense Media*, *supra* note 43; Simon, *Big Biz*, *supra* note 43; Natasha Singer, *Privacy Concerns for ClassDojo and Other Tracking Apps for Schoolchildren*, N.Y. TIMES (Nov. 16, 2014), http://www.nytimes.com/2014/11/17/technology/privacy-concerns-for-classdojo-and-other-tracking-apps-for-schoolchildren.html.

55. Singer, *supra* note 58.

56. *See, e.g.*, Diane Ravitch, *WSJ: Big Data Enters the Classroom*, DIANE RAVITCH'S BLOG (Mar. 25, 2014), http://dianeravitch.net/2014/03/25/wsj-big-data-enters-the-classroom/ [hereinafter Ravitch, *Big Data*]; MOLNAR ET AL., *supra* note 43, at 14–17. The revelation that Google "scan[ned] and indexe[d]" emails in its educational platform, Google Apps for Education, drew intense criticism and the company changed its policies within weeks of the disclosure. Benjamin Herold, *Google Under Fire for Data-Mining Student Email Messages*, EDUC. WEEK (Mar. 26, 2014), http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html; Benjamin Herold, *Google Amends Terms for Scanning User Data*, EDUC. WEEK (Apr. 23, 2014), http://www.edweek.org/ew/articles/2014/04/23/29google.h33.html.

access to, or unintentional disclosure of, student information.[57] Parents and students fear that the data will be ripe for identity theft, or that it will compromise the safety of the students by providing personal information to would-be predators.[58] They worry that sensitive information will be made public through human mistake or technological error.[59] They predict that permanent records limit students' future opportunities based on outdated, inaccurate, or irrelevant information.[60]

Advocates raise concerns about probabilistic and predictive analytics unintentionally pigeonholing underserved students.[61] Both educational and non-educational actors might use student information in ways that stigmatize or discriminate against students.[62] Many fear that for-profit interests will use and repurpose student information to maximize profits, not student welfare, or use it to inform decision-making outside the immediate education context.[63] Observers question how nontraditional entities that provide digital education platforms directly to students, but are governed by general commercial law—like Khan Academy and Coursera—will use student data.[64] Stakeholders worry that information collected in schools will be repurposed for secondary and commercial purposes, including research by providers, schools, administrators, policymakers, and learning scientists.[65]

---

57. *See, e.g.*, Herold, *Americans Worried*, *supra* note 58; Davis & Cavanagh, *supra* note 58.

58. *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/ [hereinafter Ravitch, *Identity Theft*].

59. *See, e.g.*, Megan O'Neil, *Data Breaches Put a Dent in Colleges' Finances as Well as Reputations*, CHRON. OF HIGHER EDUC. (Mar. 17, 2014), http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/ (describing a cyberattack on the University of Maryland that resulted in the theft of 309,079 student and personnel records).

60. *See, e.g.*, 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; Ravitch, *Big Data*, *supra* note 60.

61. *See* Audrey Watters, *Click Here to Save Education: Evgeny Morozov and Ed-Tech Solutionism,* HACK EDUC. (Mar. 26, 2013), http://hackeducation.com/2013/03/26/ed-tech-solutionism-morozov; Joseph Turow, *How Should We Think About Audience Power in the Digital Age?*, *in* THE INTERNATIONAL ENCYCLOPEDIA OF MEDIA STUDIES (2013).

62. *See* Watters, *supra* note 65; Turow, *supra* note 65.

63. *See* Ravitch, *Identity Theft*, *supra* note 62; Diane Ravitch, *3 Dubious Uses of Technology in Schools*, SCI. AM. (Aug. 1, 2013), http://www.scientificamerican.com/article/diane-ravitch-3-dubious-uses-technology-in-schools/; MOLNAR ET AL., *supra* note 43, at 28.

64. *See, e.g.*, Caitlin Emma, *Online Education Run Amok?*, POLITICO (Nov. 29, 2014, 8:59 AM), http://www.politico.com/story/2014/11/online-education-run-amok-113208.html; Simon, *Big Biz*, *supra* note 43.

65. *Common Sense Media*, *supra* note 43.

II. FERPA'S FOUNDATIONS

FERPA was one of the first federal laws specifically addressing systemic privacy concerns. FERPA's enactment in 1974 responded to "the growing evidence of the abuse of student records across the nation."[66] At the time, schools generally kept student records on paper in student-associated manila folders in a filing cabinet located in a school administrator's office on school premises.[67] Disclosure consisted of showing or mailing records upon request or giving out information on the phone. The "friction" of physical and verbal disclosure meant that most information schools collected about students generally remained in the immediate education environment.

Schools began collecting information beyond classes, teachers, attendance, and grades as the demand to provide a broader array of services emerged.[68] Educators, social service agencies, and educational researchers also started surveying students about their families, beliefs, values, drug use, and sexual mores to gain insight into the "whole child."[69] In the turbulence of the late 1960s and early 1970s, higher education institutions collected information on student activists and shared it with law enforcement, national intelligence, and Selective Service officials.[70]

In 1969, the Russell Sage Foundation conducted a study on student record-keeping (the "Report") that found schools provided parents and students with insufficient notice or opportunity to consent to data collection or disclosure and limited ability to access or amend student records.[71] Schools, for example, might withhold a student's IQ test results under the rationale that parental or student knowledge of this information would hinder student educational progress.[72]

---

66. 121 CONG. REC. 13,990 (1975) (statement of Sen. Buckley before the legislative conference of the National Congress of Parents and Teachers).

67. *See* Diane Divoky, *Cumulative Records: Assault on Privacy*, 2 LEARNING 18, 18–21 (1973).

68. Diane Divoky, *How Secret School Records Can Hurt Your Child*, PARADE., Mar. 31, 1974, at 4–5; RUSSELL SAGE FOUND., GUIDELINES FOR THE COLLECTION, MAINTENANCE, & DISSEMINATION OF PUPIL RECORDS: REPORT OF A CONFERENCE ON THE ETHICAL & LEGAL ASPECTS OF SCHOOL RECORD KEEPING 7 (1970) [hereinafter RUSSELL SAGE REPORT].

69. *See* RUSSELL SAGE REPORT, *supra* note 72, at 13–15; Divoky, *supra* note 71.

70. *See* Sarah C. Carey, *Students, Parents and the School Record Prison: A Legal Strategy for Preventing Abuse*, 3 J.L. & EDUC. 365 (1974) (noting that school districts in New York City granted access to student records to outside agencies and individuals such as police, FBI agents, military intelligence officers, and Selective Service board representatives).

71. RUSSELL SAGE REPORT, *supra* note 72, at 13–14.

72. *Id.* at 14.

The Report enumerated concerns about the ad hoc nature of most disclosure of student information and an absence of institutional protocols and documentation.[73] The idea of secret files creating a proverbial "permanent record" that limited students' future opportunities was particularly resonant in 1974, given the broader privacy concerns raised by the Watergate scandal.[74] Stakeholders feared that inaccurate "erroneous," "harmful," and out-of-date material in a child's records might have "devastatingly negative effects on the academic future and job prospects of an innocent, unaware student."[75]

Senator James Buckley introduced FERPA as a floor amendment to an education budget bill to remedy these "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."[76] He sought to ensure that parents could inspect and correct school and district student records. Senator Buckley also wanted to provide parents and students with more notice of and control over disclosure of potentially harmful information to outside parties,[77] especially about disclosure to possible employers, social service workers, and law enforcement officials.[78]

A. Statutory Provisions

Specifically, FERPA provides parents and students over eighteen years old or enrolled in a post-secondary education institution ("eligible students")[79] with three rights regarding personally identifiable

---

73. *Id.* at 14, 31.

74. 120 CONG. REC. 14,580 (1974) (statement of Sen. Buckley) (noting privacy concerns prompted by Watergate); Carey, *supra* note 74, at 387.

75. 120 CONG. REC. 14,580; 120 CONG. REC. 39,862–63 (1974) (statement of Sen. Buckley & Sen. Pell) (expressing the legislators' intent that, with the adoption of the Act, "parents and students may properly begin to exercise their rights under the law, and the protection of their privacy may be assured").

76. 121 CONG. REC. 39,991. Buckley submitted the article to be included in the Congressional Record. *Id*. at 13,951–53.

77. 120 CONG. REC. 39,864.

78. Divoky, *supra* note 71, at 18–21; *Students' Rights and the "Buckley Amendment,"* YOUNG SPARTACUS, Jan. 1975, at 3 (noting controversy regarding FBI surveillance of high school students).

79. The 1974 Buckley/Pell Amendment provides that these rights transfer to students over eighteen years old or enrolled in post-secondary education ("eligible students"). 120 CONG. REC. 39,865. For the purposes of this Article, references to parents in relation to FERPA and to "parents and students" identify the set of individuals eligible to grant consent under FERPA's framework.

information ("PII")[80] maintained in a student's education record.[81] They have the right to: (1) inspect and review the accuracy of the record; (2) challenge the accuracy of the record at a hearing and provide correction or commentary; and (3) prevent PII collected by the institution and maintained in the student's educational record from being disclosed to any third party without written consent.[82]

FERPA conditions federal funding of educational institutions and agencies ("educational entities")[83] on compliance with rules requiring them to provide access to and limit disclosure of PII maintained in a student's education record.[84] On request, educational entities must provide parents with access to student records[85] and a hearing to contest their accuracy.[86] Educational entities cannot share covered information with outside parties without the consent of parents or eligible students (over eighteen or enrolled in a post-secondary education institution), unless one of several exceptions applies, or the information is in a designated category of "directory information" excluded from FERPA's consent requirements.[87]

Numerous exceptions also permit educational entities to share information without requiring parent or student consent. Some excep-

80. *See* 34 C.F.R. § 99.3 (2009) ("Personally Identifiable Information … includes … [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.").

81. 20 U.S.C. § 1232g(a)–(b) (2012); 121 CONG. REC. 13,991.

82. § 1232g(a)–(b).

83. § 1232g(a)(3). Under FERPA, an educational agency or institution is "any public or private agency or institution which is the recipient of funds under any applicable program." *Id.*

84. § 1232g(a)–(b). FERPA's definition of an education record does not include: (1) records kept "in the sole possession of the maker," used only as a personal memory aid, and "not accessible or revealed to any other person except a [temporary] substitute" for the maker of the record; (2) records of the "law enforcement unit of [an] educational agency or institution" that created in its capacity as a law enforcement agency rather than a department of the school; and, (3) records relating to an individual "employed by an educational agency or institution," "made and maintained in the normal course of business that relate exclusively to [the individual] in that [individual's] capacity as an employee and are not available for use for any other purpose." § 1232g(a)(4)(B); 34 C.F.R. § 99.3 (2009).

85. § 1232g(a)(1)(A)–(a)(2). The practicality of this provision has been challenged by the proliferation of data and different data systems. In response to a recent request by a Nevada parent to review his children's records, the Nevada Board of Education indicated that it could not fulfill the request because doing so would require acquisition of $10,000 worth of technology. Benjamin Herold, *$10,000 Price Tag Put on Nevada Parent's Data Request*, EDUC. WEEK. (June 10, 2014), http://www.edweek.org/ew/articles/2014/06/11/35data.h33.html [hereinafter Herold, *$10,000 Price Tag*].

86. § 1232g(a)(2). If their challenge is not successful, parents have the right to note their challenge in the student's record. *Id.*

87. *See* 34 C.F.R. § 99.31. Note that while FERPA does not strictly "prohibit" information practices, it is commonplace to use the term in discussing its requirements. Here I use it to connote that actors engaging in prohibited activities will not qualify for federal funding.

tions enable educational entities to comply with judicial and executive branch requirements and respond quickly when students' health or security is at risk.[88] Other exceptions permit nonconsensual disclosure to certain education-related recipients to reduce educators' administrative burdens in helping students progress through the education system.[89] These are based on the roles recipients play within the education system. These include sharing information with schools or school systems for purposes related to a student's application for admission or transfer,[90] in connection with processing financial aid applications,[91] or required by accrediting organizations.[92] Most controversially, these exceptions also allow educational institutions and agencies to share covered information with outside entities performing services, conducting studies, or facilitating evaluation and required reporting on their behalf.[93]

FERPA confers no private right of action.[94] Instead, the DOE has the power to withdraw all public funding of an educational institution with a "policy or practice" of FERPA violation.[95] Because the statute connects to federal spending, it only applies to educational agencies or institutions that receive funds from the DOE, either directly via grant, or indirectly through students. This includes institutions with students awarded federal financial aid and encompasses nearly all private and public elementary and secondary schools, colleges, and universities.[96] The DOE has never exercised its discretion

88. Secretary of Education Arne Duncan has noted that "FERPA allows disclosure without consent because there are essential and legitimate educational needs to disclose data where parental control cannot be reasonably implemented . . . such as when a school district is disclosing PII from education records on its students to a contractor to operate the district's student records system." Letter from Arne Duncan, Secretary of Education, to Edward J. Markey, U.S. Senator 3–4 (Jan. 13, 2014), *available at* http://www2.ed.gov/about/offices/list/om/docs/pirms/edrespmarkey.pdf.

89. *See* § 99.31.

90. § 99.31(a)(3)(ii)(2).

91. § 99.31(a)(3)(ii)(4)(i).

92. § 99.31(a)(3)(ii)(7).

93. § 99.31(a)(6)(i); FERPA's other exceptions to consent include: schools a student is transferring to; accrediting organizations; financial aid-related entities; and in cases of a health and safety emergency or to investigate or prosecute terrorism under the Patriot Act. *Id.*

94. Gonzaga Univ. v. Doe, 536 U.S. 273, 290 (2002).

95. 20 U.S.C. § 1232g(b)(1)–(2) (2012). Pursuant to subsequent amendments, the DOE can prohibit an educational institution from sharing information for five years with third parties found in violation of certain FERPA requirements. 34 C.F.R. § 99.67 ("If the Office finds that a third party, outside the educational agency or institution, violates [the PII disclosure provision], then the educational . . . institution from which the personally identifiable information originated may not allow the third party . . . access to [PII] . . . for at least five years.").

96. *See* § 1232g(a)(3); 34 C.F.R. § 99.1(a)(1)–(2) (2000) (defining educational agencies and institutions in terms of funding received and services provided).

to withdraw federal funding for FERPA violations in the statute's forty-year history.[97]

B. FERPA's Delegation-Based Privacy Regime

FERPA seeks to impose structure and procedure upon educational institutions and agencies to reduce undocumented, ad hoc, and inconsistent decision-making regarding sharing information in student records with outside parties. Its default provisions focus on enabling privacy self-management through notice, consent, access, and amendment provisions.[98] These align with FIPPs,[99] the widely accepted framework[100] of defining principles used to create and evaluate systems, processes, and programs that affect individual privacy.[101]

In practice, however, FERPA creates a structure in which institutions, not individuals, manage student privacy. The statute's exceptions to consent reflect a baseline trust in educational actors' internal information practices and authority to determine when disclosure of student PII prevents imminent danger, serves a student's educational interests, or is required by institutional needs. It only defers to parents' privacy preferences regarding disclosure, while giving educational actors almost complete authority over data collection, secu-

97. *Joel Reidenberg on FERPA Overhaul*, FORDHAM L. NEWS (Apr. 28, 2015), http://news.law.fordham.edu/blog/2015/04/28/joel-reidenberg-on-ferpa-overhaul/.

98. Family Educational Rights and Privacy, 76 Fed. Reg. 75,604, 75,605 (Dec. 2, 2011) (to be codified at 34 C.F.R. pt. 99).

99. While the articulation of these principles varies, they generally consist of principles that prohibit secret record-keeping systems; enable individuals to find out information about themselves in a record and how it is used; allow individuals to prevent information obtained for one purpose from being used for another; allow individuals to correct records about themselves; and require organizations creating the record to assure its reliability and take steps to prevent misuse. *See* Robert Gellman, *Fair Information Practices: A Basic History*, BOB-GELLMAN.COM (Feb. 11, 2015), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. These were originally referred to as Fair Information Practices, but I use the more common, contemporary reference.

100. FERPA's regulatory regime is unusual among federal privacy statutes because it predates the Privacy Act of 1974, which marked the adoption of Fair Information Practice Principles (FIPPs) as guidelines and requirements for appropriate information flow. Accordingly, FERPA does not formally align with, but incorporates some of, these principles—most notably through provisions for notice and consent to disclosure and the right to access and amend covered information. *See* Gellman, *supra* note 103.

101. U.S. DEP'T. OF HEALTH, EDUC. AND WELFARE, DHEW NO. OS 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS viii (1973); Gellman, *supra* note 103; s*ee also* HUGO TEUFEL III, U.S. DEP'T OF HOMELAND SEC., MEMORANDUM NO.: 2008-01, PRIVACY POLICY GUIDELINE MEMORANDUM (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

rity, use, and retention.[102] Rather than deferring to user privacy preferences, FERPA creates a framework that gives parents and students few opportunities to exercise control over information disclosure while affording educational entities considerable discretion and minimal obligation to be transparent regarding the procedure, criteria, and record-keeping surrounding these decisions.

C. Delegation Under FERPA's School Official Exception

FERPA's delegation of decision-making to educational institutions is particularly evident, and controversial, in the School Official Exception that governs most of the information disclosed by schools to outside parties that provide learning apps, email, and information management systems. The exception permits schools to share data—without consent—to a "school official" who (1) "[p]erforms an institutional service or function" for which employees otherwise would be used; (2) the school or district has determined to have "legitimate educational interests" in the education records, as defined by the school or district in its annual notification of FERPA rights; and (3) does not re-disclose covered PII unless it is shared "with the understanding" she or he may do so on the educational institution's behalf.[103]

Educational actors have broad discretion and minimal transparency obligations under the exception. They determine the criterion

102. A significant amount of potentially sensitive student information falls outside the statute's protection due to narrow definitions of what constitutes PII maintained in a student's education record and an exclusion for institutionally-defined "directory information." *See* 20 U.S.C. § 1232g(a)(5)(A) (2012). In recent non-binding guidance, the DOE has implicitly acknowledged that FERPA protection excludes important types of data collected about students by recommending educational institutions and agencies protect a broader definition of "sensitive" rather than "personal" information. U.S. DEP'T OF EDUC., *Data Security Checklist*, PRIVACY TECHNICAL ASSISTANCE CTR. 5 (last visited Apr. 18, 2016), http://nces.ed.gov/programs/ptac/pdf/ptac-data-security-checklist.pdf (defining sensitive information as "data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII"). *See* Erika McCallister et al., NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T. OF COMMERCE, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 2-1 n.14 (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. Discussion of the scope of information FERPA protects is beyond the purview of this Article.

103. 34 C.F.R. § 99.31(a)(B)(1) (2015); 34 C.F.R. § 99.33 (use and re-disclosure requirements); U.S. Dep't of Educ., *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, PRIVACY TECH. ASSISTANCE CTR. 3–4 (Feb. 2014) [hereinafter *Protecting Student Privacy*], *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf.

for who constitutes a school official and what constitutes a legitimate educational interest, and must include this information in an annual FERPA notice.[104]

When FERPA was enacted, the actors likely to be school officials included educational actors, such as substitute teachers or parent volunteers.[105] The School Official Exception sought to prevent these intra-institutional actors from accessing personally identifiable student information simply to satisfy curiosity or serve personal motives unrelated to the educational enterprise.[106] It also sought to limit ad hoc decision-making about periodic disclosure to outside actors like law enforcement officers or social workers.[107]

FERPA did not explicitly address schools' routine sharing information with extra-educational actors until recently. As schools began to share information with outside data recipients more routinely, the DOE amended the exception to include explicit "outsourcing" provisions.[108] The 2008 changes expanded the definition of "school officials" to include "contractor[s], consultant[s], volunteer[s], and other part[ies] to whom an [educational] agency or institution has outsourced institutional services or functions" it would otherwise use employees to perform.[109]

1. Informal designation of school official status

Disclosure under the School Official Exception is informal. FERPA does not specify how schools must determine who is an appropriate data recipient, how to document this approval, or the scope of such

104. 34 C.F.R. § 99.7(a)(3)(iii) (2015).

105. U.S. Dep't of Educ., Model Notification of Rights Under FERPA for Elementary and Secondary Schools (last modified Dec. 22, 2014), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html; see also U.S. Dep't of Educ., Model Notification of Rights Under FERPA for Postsecondary Institutions (last modified Jan. 2, 2015), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html.

106. 34 C.F.R. § 99.31(a)(1)(ii) (2015) ("An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those educational records in which they have legitimate educational interests.").

107. 121 CONG. REC. 13,990 ("Access to pupil records by non-school personnel and representatives of outside agencies is, for the most part, handled on an ad hoc basis. Formal policies governing access by law-enforcement officials, the courts, potential employers, colleges, researchers and others do not exist in most school system [sic].").

108. *Family Educational Rights and Privacy Act Final Rule 34 CFR Part 99: Section-by-Section Analysis* 5 (Dec. 2008), http://www.wrightslaw.com/law/ferpa/finalrule.sec.analysis.08.pdf; Family Educational Rights and Privacy Regulations Notice of Proposed Rulemaking, 76 Fed. Reg. 75,604, 75,607 (Dec. 2, 2011) [hereinafter FERPA 2008 DOE Analysis].

109. 34 C.F.R. § 99.31(a)(1)(i) (2015); Family Educational Rights and Privacy Regulations Notice of Proposed Rulemaking, 73 Fed. Reg. 74,806, 74,852 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99).

authorization.[110] It does not require any formal designation of school official status, specification of the purposes served by disclosure, or a threshold data security and governance mechanism.[111]

Schools' and districts' data practices do not have to document disclosure to school officials.[112] Accordingly, many schools do not have explicit policies regarding classroom adoption of technologies that use covered student information.[113] Teachers, for example, may share covered information with free apps without any documentation or institutional oversight.[114]

2. Broad discretion over security and approval of data recipients

FERPA requires minimal oversight of data recipients or security requirements. At a minimum, educational institutions must ensure that school officials, including school and district employees, can only access student information if there is a legitimate educational interest in doing so.[115] The new outsourcing provisions require educational institutions to use "reasonable methods" to exercise "direct control" over these parties to ensure a data recipient's information practices are FERPA-compliant.[116] A contract between the parties may satisfy these requirements.[117] However, while DOE guidance

---

110. *See Protecting Student Privacy*, *supra* note 107, at 3–5.

111. *Id.* at 8 ("When possible, use a written contract or legal agreement.").

112. 34 C.F.R. § 99.32(d)(2) (2015).

113. Michele Molnar, *Ed. Industry Groups Outline Steps to Protect Privacy of Student Data*, EDUC. WEEK (Apr. 14, 2014), http://www.edweek.org/ew/articles/2014/04/16/28privacypractices.h33.html?tkn=UNUF%2F1EFFJmmhWmx%2F5tMKTKzagiU50zJ5bTn&print=1.

114. *See, e.g.*, Barnes & Strauss, *supra* note 2; *How Emerging Technology Affects Student Privacy: Hearing Before the H. Comm. on Educ. and the Workforce*, 114th Cong. 3–4 (2015) (statement of Joel R. Reidenberg, Professor, Fordham University School of Law), *available at* http://edworkforce.house.gov/uploadedfiles/reidenberg_testimony_final.pdf; *How Data Mining Threatens Student Privacy*: Hearing Before the H. Comm. on Homeland Security Subcomm. on Cybersecurity, Infrastructure Prot. and Sec. Tech. and Comm. on Educ. and the Workforce Subcomm. on Early Childhood, Elementary and Secondary Education, 113th Cong. 2 (2014) (statement of Joel R. Reidenberg, Professor, Fordham University School of Law), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg91448/html/CHRG-113hhrg91448.htm.

115. 34 C.F.R. § 99.31(a)(1) (2015).

116. § 99.31(a)(1)(ii) (stating that schools must use "reasonable methods" to ensure that school officials obtain access only to those education records in which they have legitimate educational interests); 34 C.F.R. § 99.67; § 99.31(1)(B)(2) (noting that recipients "must be under the direct control of the disclosing institution and subject to the same conditions on use and redisclosure of education records that govern other school officials"). *See also* Duncan, *supra* note 92, at 3.

117. *Protecting Student Privacy*, *supra* note 107, at 4 ("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. In some cas-

suggests schools and districts control "web-based and email services . . . [through] contracts," it is not a requirement.[118] Educational agencies and institutions do not have to record specific disclosures of directory information pursuant to the transfer or school official exceptions as long as they indicate their general practices in an annual FERPA notice.[119]

The standards for "reasonable methods" or "direct control" are loosely defined in non-binding guidance.[120] The DOE suggests the reasonableness should correspond to the magnitude of harm presented by different types of information and reflect the customary practices of similarly-situated institutions.[121] It has promulgated best practices, but leaves the details of safeguarding student information to the institutions themselves to ensure such requirements are "sufficiently flexible" to account for varying resources and needs.[122]

3. Predominantly procedural purpose limitations

Although schools must set forth the criteria for who is considered a school official in their annual FERPA notices, there is little substantial constraint on institutional discretion. The DOE's model FERPA notices for lower and higher education suggest the following language:

> A school official typically includes a person employed by

---

es, the 'Terms of Service' (TOS) agreed to by the school or district, prior to using the online educational services, may contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements.").

118. Family Education Rights and Privacy Regulations, 73 Fed. Reg. 74,806, 74,816 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99). For example, the DOE suggests that schools outsourcing information technology services use contract provisions to restrict third parties from using or allowing access to PII from education records "except in accordance with the requirements established by the educational agency or institution that discloses the information." *Id.*

119. § 99.31(a). If an educational entity discloses information under these exceptions with the understanding that data recipients can re-disclose information on their behalf, the record must also list approved additional recipients and the legitimate interest that they have in requesting or obtaining the information. § 99.33(b)(1); § 99.32(a)(3)(ii).

120. *See* U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., GUIDANCE FOR REASONABLE METHODS AND WRITTEN AGREEMENTS, 4–6 (2015), *available at* http://ptac.ed.gov/sites/default/files/Guidance_for_Reasonable_Methods%20final.pdf.

121. *See id.*

122. *See id.*; U.S. DEP'T OF EDUC., SAFEGUARDING STUDENT PRIVACY (2011), *available at* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/safeguarding-student-privacy.pdf; Family Education Rights and Privacy Regulations, 73 Fed. Reg. 74,806, 74,817 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99) ("We believe that the standard of 'reasonable methods' is sufficiently flexible to permit each educational agency or institution to select the proper balance of physical, technological, and administrative controls to effectively prevent unauthorized access to education records, based on their resources and needs.").

> the school or school district as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer, contractor, or consultant who, while not employed by the school, performs an institutional service or function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks.[123]

Educational institutions have almost universally adopted similar language.[124]

FERPA gives schools similarly broad scope and considerable deference in determining what constitutes a legitimate educational interest required to share information with a school official. As noted by the National Center for Education Statistics, the statute "does not say specifically who those persons are, nor does it stipulate how to determine the limits of a legitimate educational interest."[125] Nor does it specify whether disclosure should serve the legitimate educational interest of the student data subject, the institution, or learn-

123. Model Notification of Rights Under FERPA for Elementary and Secondary Schools, *supra* note 109; *see also* Model Notification of Rights Under FERPA for Postsecondary Institutions, *supra* note 109.

124. For example, New York University's FERPA notice states, "school officials having a legitimate educational interest include any University employee acting within the scope of her or his University employment, and any duly appointed agent or representative of the University acting within the scope of his or her appointment." *New York University Guidelines For Compliance With FERPA*, N.Y.U. (Sept. 2013), http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/FERPA.html [hereinafter *New York University Guidelines*].

125. NAT'L CTR. FOR EDUC. STATISTICS, FORUM GUIDE TO PROTECTING THE PRIVACY OF STUDENT INFORMATION: STATE AND LOCAL EDUCATION AGENCIES 51 (Mar. 2004), http://nces.ed.gov/pubs2004/2004330.pdf; *see also* § 99.31(a)(1)(ii) (2015).

ers generally.[126] Legitimate educational interests do not even have to relate to academic or educational matters.[127]

Following DOE guidance, most institutions define "legitimate educational interest" in terms of functionality rather than substantive criteria.[128] The DOE's model FERPA notices state that a "school official typically has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilit[ies]" for the educational institution.[129]

Beyond this, there is minimal guidance, except for advice buried in the DOE's answers to specific institutional queries on student privacy. These indicate, for example, that the educational interest of an individual was sufficient to justify disclosure in certain circumstances, but that a professor's curiosity was not in others.[130] Given the minimal statements scattered throughout these responses, however, it is conceivable that almost "[a]nything relevant to a school official's job may be a legitimate educational interest."[131]

While the discretion to define what constitutes a legitimate educational interest is not limitless, the DOE defers to educational institutions' determinations.[132] This stance aligns with long-standing defer-

126. *See* § 99.31(a)(1)(ii); Control of Access to Education Records by School Officials, 73 Fed. Reg. 237, at 74,817 ("Thus, a district or institution that makes a disclosure solely on the basis that the individual is a school official violates FERPA if it does not also determine that the school official has a legitimate educational interest.").

127. Nancy Tribbensee, *Privacy and Confidentiality: Balancing Student Rights and Campus Safety*, 34 J.C. & U.L. 393, 400 (2008) ("A legitimate educational interest is not strictly limited to academic or educational matters, and permitted disclosures are not limited to those that may address the student's interest or that may be to the benefit of the student.").

128. *See, e.g.*, FAIRFAX COUNTY PUBLIC SCHOOLS, OFFICE OF THE SUPERINTENDENT, MANAGEMENT OF THE STUDENT SCHOLASTIC RECORD: STUDENT SCHOLASTIC RECORDS MANUAL (Aug. 2015), http://www.fcps.edu/is/schoolcounseling/documents/ssrm.pdf; *see also* EASTERN CONNECTICUT STATE UNIVERSITY, ANNUAL NOTICE OF RIGHTS UNDER FERPA (Aug. 25, 2014), http://www1.easternct.edu/registrar/files/2014/10/Annual-Notice-of-Rights-under-FERPA-Fall-2014.pdf.

129. Model Notification of Rights Under FERPA for Elementary and Secondary Schools, *supra* note 109; *see also* Model Notification of Rights Under FERPA for Postsecondary Institutions, *supra* note 109.

130. *See* Letter from LeRoy S. Rooker, Family Policy Compliance Office, U.S. Dep't of Educ., to Dr. John R. Leitzel, President, University of New Hampshire (Jan. 31, 2001), *available at* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/unh.html; *see also* NAT'L CTR. FOR EDUC. STATISTICS, FORUM GUIDE TO PROTECTING THE PRIVACY OF STUDENT INFORMATION: STATE AND LOCAL EDUCATION AGENCIES, DEFINING "LEGITIMATE EDUCATIONAL INTERESTS, *available at* http://nces.ed.gov/pubs2004/privacy/section_4b.asp (last visited Apr. 18, 2016).

131. Robert Steinbuch, *Four Easy Pieces to Balance Privacy and Accountability in Public Higher Education: A Response to Wrongdoing Ranging from Petty Corruption to the Sandusky and Penn State Tragedy*, 46 LOY. L.A. L. REV. 163, 180 (2012) (quoting Daniel Silverman, *Student Privacy Versus Human Rights*, 35 HUM. RTS. 9, 10 (2008)).

132. The National Center for Education Statistics has suggested that the DOE "could rule, as a matter of law, that a school official did not have 'legitimate educational interest' in access-

ence to educational institutions' decisions, following the historically local control of the public education system and traditional autonomy accorded to higher education institutions in the name of academic freedom.[133]

In practice, the bounds of what constitute an appropriate "school official" data recipient and "legitimate educational interest" are nebulous at best. Current definitions in annual FERPA notices merely reiterate the existing requirements of the School Official Exception. They convey that school official status turns on whether the data recipients perform services that would otherwise be performed by an employee, and that a legitimate interest exists when the recipient uses student information to perform functions on behalf of the educational institution.[134] These create primarily procedural, rather than substantive, requirements and a somewhat circular dependence on institutional approval. In essence, the act of an educational actor providing access to student information to a recipient performing some function for an educational actor is sufficient to satisfy the statute on its face. Accordingly, FERPA-compliant disclosure still permits a broad scope of data practices that may only serve legitimate educational interests indirectly or of the institution rather than the student data subject.

4. Contextualized criteria for compliance

Recent DOE guidance to schools outsourcing information to online providers highlights the broad discretion educational agencies and institutions have under FERPA's purview.[135] The guidance is helpful as a promulgation of norms and best practices, but provides few bright line rules.[136] It instead answers several questions about the propriety of particular practices with "[i]t depends," and

---

ing information contained in education records." *See, e.g.*, NAT'L CTR. FOR EDUC. STATISTICS, *supra* note 129, at 51.

133. DAVID F. LABAREE, SOMEONE HAS TO FAIL: THE ZERO-SUM GAME OF PUBLIC SCHOOLING 69–70 (2012); *see also* Frederick P. Schaffer, *A Guide to Academic Freedom*, TRUSTEESHIP 8 (Apr. 2011), *available at* http://agb.org/trusteeship/2011/julyaugust/a-guide-to-academic-freedom ("[T]he Supreme Court has at a various times recognized that . . . the institutional autonomy of universities and the rights of faculty [sic] are part of academic freedom.").

134. *See, e.g.*, *New York University Guidelines*, *supra* note 128 ("[S]chool officials having a legitimate educational interest include any University employee acting within the scope of her or his University employment, and any duly appointed agent or representative of the University acting within the scope of his or her appointment.").

135. *Protecting Student Privacy*, *supra* note 107, at 2–3.

136. *Id.*

notes that educational entities' obligations under the statute depend on case-specific circumstances.[137]

The guidance uses examples to illustrate its points, which obscure the determinative factor in many instances.[138] Most of the examples also operate under the questionable assumption that schools share information with data recipients under auspices of a written agreement that articulates, in particular, the specific services and purposes for which the information has been shared.

One example notes that an outside party who provides online tutoring services and accesses information under the School Official Exception can use FERPA-covered information to personalize learning modules for the educational institution's students.[139] The DOE explains that this is because the tutoring provider was "only using FERPA-covered information for the purposes for which it was shared."[140] The guidance also states that third party providers can use PII to improve products as long as they are not solely for the purpose of developing products never intended for the school's use.[141]

The bounds of this prohibition are unclear. If framed as a permissive, rather than restrictive principle, does this example permit repurposing designed in part to develop products that the school could use? How does this apply to research used to analyze market needs that may or may not correspond to those of the data-sharing institution? How does it inform algorithms that may or may not be refined in time to be incorporated into or turn out to be irrelevant to the services provided to that specific school?

Other examples state that third parties cannot use FERPA-covered information for "different purposes than those for which the data was shared" (cafeteria management services targeting students with food advertising) or purposes that were "not authorized by the district and do[]not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights" (email provider serving students targeted advertisements for toys).[142]

The basis for these is also unclear. In both cases, the third party's secondary use of student information fell outside of the purposes for disclosure authorized by the educational institution. This implies

137. *Id.* at 3.
138. *Id.*
139. *Id.* at 6.
140. *Id.*
141. *Id.* at 7.
142. *Id.* at 5, 7.

that the educational institution authorized the outside party to use information for specific purposes. What happens in the absence of specific authorization? The restriction on third party re-disclosure does not apply if the information is provided "with the understanding" that the recipient may disclose on the educational institution's behalf.[143] If, for example, a teacher shares covered information pursuant only to a company's wrap privacy policies, which include provisions describing the companies' distribution of information to subcontractors and other affiliates, one could argue that the necessary understanding is in place.

The example also provides little guidance about using information for secondary purposes. Would it matter if the targeted advertising promoted supplemental tutoring apps that students might use instead of toys? Does the compound explanation mean that either factor alone would not violate FERPA?

A final example involves a teacher disclosing student photographs through an independently downloaded app whose clickwrap terms of service permit the app's "provider[s] to use the information for a variety of non-educational purposes, including selling merchandise."[144] The district discovered these practices, and determined that the app's terms of service violated FERPA.[145] This example, as well as the toy-marketing example, turns on violations of institutionally defined legitimate educational interests. The district determines whether the use was outside its definition of a legitimate educational interest. This does not suggest that the use is unacceptable overall. Could another district decide that targeting toy advertising did serve a legitimate educational interest because it helped children develop spatial skills? Or that selling student information to raise funds for new textbooks served a legitimate educational purpose?[146]

While these examples provide excellent guidance regarding best practices, upon closer examination they highlight the statute's delegation-based regulatory model. In a regulatory structure where au-

143. 34 C.F.R. § 99.33(b)(1) (2014).

144. *Protecting Student Privacy*, *supra* note 107, at 11.

145. *Id.*

146. I do not mean to suggest that PTAC, which issued these guidelines, used very specific examples out of incompetence or political motive. The careful construction of the Center's guidance documents reflects an awareness of, and attempt to ameliorate, the types of concerns FERPA does not address, but also the reality that the current regulatory regime gives the DOE only a very limited ability to do so. PTAC's non-binding guidance and best practices still have significant value as models for educational institutions to follow and establish information norms that encourage voluntary adoption by schools and districts.

thorization is akin to legitimatization, and deference is afforded to educational actors' decision-making, this flexibility would permit schools to share student information for virtually unlimited purposes as long as they could provide a justification that furthered a legitimate educational interest. This could, in theory, include selling student information to raise funds to purchase items like school supplies or textbooks.

5. Compliance-oriented enforcement

Upon finding a violation, the Family Policy Compliance Office (FPCO) of the Department of Education notifies the institution, which then has "a reasonable period of time" to comply voluntarily with its FERPA obligations.[147] If the entity does not comply, the FPCO can initiate "any legally available enforcement action" to compel compliance.[148] This compliance-oriented approach ensures that institutions have policies and practices in place to prevent the ad-hoc disclosure of student information, and not simply account, or provide redress, for individual violations. At a practical level, this limits enforcement to the unlikely case of an educational institution intentionally and repeatedly violating FERPA after FPCO attempts to bring it into compliance.[149]

Because FERPA is a spending clause statute, the main enforcement mechanism available to the DOE is complete withdrawal of federal funds.[150] However, the Department of Education has never imposed this dramatic—and potentially catastrophic—measure over the course of the statute's forty-year history.[151] Doing so would likely have dire institutional consequences, and ultimately harm the students that FERPA seeks to protect. Accordingly, absent egregious circumstances, FERPA's enforcement may be an empty threat.[152]

---

147. *See* 34 C.F.R. § 99.66(c)(2) (2012).

148. 34 C.F.R. § 99.67(a) (2012).

149. *See* Stephanie Humphries, Note, *Institutes of Higher Education, Safety Swords, and Privacy Shields: Reconciling FERPA and the Common Law*, 35 J.C. & U.L. 145, 157–58 (2009).

150. *See* 20 U.S.C. §§ 1232g(a)(1)(A)–(B), 1232g(b)(1)–(2) (2015) (stating that funds shall not be made available under any applicable program to educational agencies or institutions that have a policy or practice of denying or effectively preventing the exercise of rights assured under FERPA or of permitting the release of educational records without written consent).

151. Mary Margaret Penrose, Note, *In the Name of Watergate: Returning FERPA to Its Original Design*, 14 N.Y.U. J. LEGIS. & PUB. POL'Y 75, 107 (2011).

152. Daniel Solove, *Big Data and Our Children's Future: On Reforming FERPA*, SAVEGOV (May 6, 2014), http://safegov.org/2014/5/6/big-data-and-our-children%E2%80%99s-future-on-reforming-ferpa.

6. Limited regulatory scope

As noted above, FERPA only applies to educational agencies or institutions that receive federal funds. It does not apply to the data recipients themselves or to entities, like Massive Open Online Courses (MOOCs) that collect and use information about students independent of federally funded educational actors.[153] If the data recipient violates FERPA, the disclosing school or district is responsible for the noncompliance.[154] At most, the DOE can prohibit a publicly funded institution or agency from providing information to an entity found in violation of FERPA for at least five years.[155]

D. Delegation by Design

The delegation of decision-making to educational institutions and agencies is neither accidental nor incidental. FERPA embodies the traditional expectation that the education system would keep information it generates confidential and that condoned actors would use the information to benefit students and serve educational purposes. The statute's exceptions to consent reflect a baseline trust in educational actors' internal information practices and authority to determine when disclosure of student PII prevents imminent danger, serves a student's educational interests, or satisfies institutional needs. This is in stark contrast to the commercial sphere, which presumes that actors have conflicting, often antagonistic goals.

FERPA's model of institutional information management and compliance-oriented enforcement also accommodates highly contextualized decision-making among a radically decentralized and extraordinarily heterogeneous array of educational entities.[156] The need for a flexible framework became apparent even before FERPA's enactment.[157] In 1974, educators and educational institu-

153. *See, e.g.*, Daniel Solove, *Interview with Kathleen Styles, Chief Privacy Officer, U.S. Department of Education,* SAVEGOV (Apr. 18, 2013), http://www.safegov.org/2013/4/18/interview-with-kathleen-styles,-chief-privacy-officer,-us-department-of-education (noting that "FERPA does permit schools and school districts to contract for secure cloud services," often under the School Official Exception).

154. *See Dear Colleague Letter About Family Educational Rights and Privacy Act (FERPA) Final Regulations,* U.S. DEP'T OF EDUC. (Jan. 8, 2014), http://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht12-17-08.html ("The regulations also clarify that educational agencies and institutions are responsible for outside service providers' failures to comply with applicable FERPA requirements.").

155. 34 C.F.R. § 99.67(c)–(e) (2015).

156. *See supra* Part II.C.4–5.

157. *See generally* Carole M. Mattessich, *The Buckley Amendment: Opening School Files for Student and Parental Review*, 24 CATH. U. L. REV. 588 (1975).

tions strongly criticized and campaigned against FERPA's enactment. They predicted its provisions would be bureaucratically paralyzing and intellectually crippling.[158] At least six major higher educational institutions challenged the amendment.[159] Congress amended central FERPA provisions almost immediately after its enactment to accommodate the need for institutional information management in the education system.[160]

After House and Senate Committees reviewed the statute, Senator James Buckley successfully introduced a Joint Amendment with Senator Claiborne Pell to address stakeholder concerns.[161] The Joint Amendment gave educational institutions and agencies authority to determine what constitutes an education record rather than enumerate specific types of information that FERPA covers by substituting the broadly construed "education record" for a "laundry list" of specifically protected records.[162] The Joint Amendment also created an exclusion for institutionally defined "directory information" that could be released unconditionally unless a parent or student opted out altogether.[163] Under FERPA, directory information is information "generally [not] considered harmful or an invasion of privacy if disclosed[,]" including students' names, addresses, phone numbers, email addresses, dates and places of birth, photographs,

158. ALFRED B. FITT, A SPECIAL REPORT FROM THE WASHINGTON OFFICE OF THE COLLEGE ENTRANCE EXAMINATION BOARD (Jan. 3, 1975), *reprinted in* HIGHLAND CAVALIER, Jan. 27, 1975, at 2–3; *see also* Edward B. Fiske, *School Data Law Draws Criticism*, N.Y. TIMES, Oct. 13, 1974, at 46.

159. Mattessich, *supra* note 161, at 597; Fiske, *supra* note 162 (discussing how chief executives at six major higher education institutions requested delaying FERPA's effective date in order to provide for hearings to prevent unintended consequences).

160. *See* 120 CONG. REC. 39,862.

161. *Id.* ("[The amendment was] not intended to overturn established standards and procedures for the challenge of substantive decisions made by the institution.").

162. *Legislative History of Major FERPA Provisions,* U.S. DEP'T OF EDUC., http://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html (last modified Feb. 11, 2004). FERPA originally protected PII in:

> [A]ny and all official records, files, and data directly related to their children, including all material that is incorporated into each student's cumulative record folder, and intended for school use or to be available to parties outside the school or school system, and specifically including, but not necessarily limited to, identifying data, academic work completed, level of achievement (grades, standardized achievement test scores), attendance data, scores on standardized intelligence, aptitude, and psychological tests, interest inventory results, health data, family background information, teacher or counselor ratings and observations, and verified reports of serious or recurrent behavior [patterns].

Id. It now protects "those records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational agency or institution or by a person acting for such agency or institution." *Id.*

163. 34 C.F.R. §§ 99.31(a)(11), 99.37 (2012).

weights and heights of athletes, degrees, and awards.[164] The exclusion was designed to accommodate day-to-day administration and traditional practices, such as sending grades home to parents, using student photos in yearbooks, and disclosing athletes' statistics like weight and height in newspaper reports.[165]

The amendment required less transparency and oversight of institutional information by employing annual notices instead of requiring parental notice and consent to specify the records, reasons, and data recipients of disclosure.[166] It also gave schools the authority to make substantive decisions on what satisfied the "legitimate educational interest" standard when sharing information with recipients who provided services to schools.[167] Finally, the amendment loosened FERPA's accountability provisions by conditioning enforcement on whether educational institutions and agencies have a "policy or practice" of noncompliance.[168]

As described above, the 2008 amendments recognized the difficulty of educational institutions and agencies having direct control over remote service providers by creating the outsourcing exception. Amendments in 2008 and 2011 changed the requirements for non-consensual disclosure under the studies and audit and evaluation exceptions, which are used predominantly to accommodate state education agencies that outsource research, compliance with reporting requirements, and the creation of State Longitudinal Data Systems. This new model eschews the requirement that educational entities[169] have direct control over data recipients in favor of contractual provisions between the parties.[170] Instead, the disclosing entity requires the recipient, pursuant to a written agreement, to use reasonable methods to protect student information, only use information for the authorized purpose, and destroy the information when it is no longer needed.[171]

The comments accompanying these amendments emphasize allowing educational institutions to make contextualized decisions

164. 34 C.F.R. § 99.3 (2012) (citing 20 U.S.C. § 1232g(a)(5)(A) (2015)).

165. §§ 99.31(a)(11), 99.37; *see also Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information*, U.S. DEP'T OF EDUC. (Dec. 19, 2014), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html.

166. 120 CONG. REC. 39,863.

167. *Id.* at 39,865.

168. *Id.*

169. § 99.31.

170. Family Educational Rights and Privacy, 76 Fed. Reg. 75,604, 75,617 (Dec. 2, 2011) (to be codified at 34 C.F.R. pt. 99).

171. 34 C.F.R. § 99.35(a) (2012).

about appropriate information practices.[172] In responding to public comments to proposed regulations, the DOE states that it did not define "reasonable methods" or impose specific security and governance standards because "[i]t is important to allow for flexibility based on individual circumstances" given the "variations in conditions from school-to-school."[173] Many observers have criticized these amendments as weakening, not strengthening, protection of student information by substituting contractual provisions for direct control and oversight.[174]

III. DISMANTLING PRESUMPTIONS OF FERPA'S DELEGATION MODEL

Although FERPA provided minimal transparency and individual control over information, stakeholders tolerated its delegation of decision-making authority for almost forty years. Its framework sufficed to reassure stakeholders that student information flowed in accordance with contextual norms: that data generated by and collected from students in the course of providing education would be kept confined within the immediate education environment, to approved recipients, and to supporting a student data subject's educational attainment.[175] This section examines how new information practices have upset the underlying principles that made FERPA's student privacy protections acceptable for almost forty years. In doing so, it highlights the practices that raise the strongest concerns and, accordingly, promises focal points for meaningful reform.

---

172. Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,817 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99) ("We believe that the standard of 'reasonable methods' is sufficiently flexible to permit each educational agency or institution to select the proper balance of physical, technological, and administrative controls to effectively prevent unauthorized access to education records, based on their resources and needs.").

173. *Id.*

174. *See* Electronic Privacy Information Center, EPIC v. The U.S. Department of Education: *Challenging the Dept. of Education's Family Educational Rights and Privacy Act (FERPA) 2011 Regulations*, EPIC.ORG, http://epic.org/apa/ferpa (last visited Apr. 18, 2016); *see also* Diane Ravitch, *Why Is the US Department of Education Weakening FERPA?*, DIANE RAVITCH'S BLOG (Apr. 8, 2013), http://dianeravitch.net/2013/04/08/why-is-the-us-department-of-education-weakening-ferpa (summarizing the Electronic Privacy Information Center's lawsuit against the U.S. Department of Education); *see generally* Elec. Privacy Info. Ctr. v. U.S. Dep't of Educ., 48 F. Supp. 3d 1 (D.D.C. 2014) (challenging the 2011 amendments to FERPA).

175. *See Elec. Privacy Info. Ctr*, 48 F. Supp. 3d at 10. Institutional uses included supporting academic mobility and advancement; facilitating institutional administration; and serving core accrediting, evaluation, reporting, and legal functions within the broader education system. *Id.*

The efficacy of FERPA's regulatory mechanisms depends on several assumptions about information that no longer apply in an era of cloud computing and big data. FERPA relies on the practical obscurity of physical records to provide sufficient security against unauthorized access. FERPA's protections also rest on a presumption that sharing information requires active human effort, so that disclosure generally occurs pursuant to some conscious oversight, and, presumably, approval. In focusing on limiting disclosure as a means to prevent misuse and mismanagement of student information, the statute also operates under a tacit presumption that educational actors would use student data wisely and well.

New technology and information practices—notably the routine disclosure of student information to cloud-based service providers—raise concerns about unauthorized and involuntary disclosure, information misuse and mismanagement, and repurposing by private actors to serve non-educational purposes. With the diffusion of cloud computing, big data analytics, and educational entities' reliance on outside parties to provide data-driven services, stakeholders can no longer rely on these presumptions to ensure appropriate flow of student data. FERPA did not contemplate a world in which portable information could be put to endless purposes by educational and non-educational entities. It uses approval as the mechanism to determine whether a data recipient is appropriate, which no longer provides meaningful oversight when educational actors can disclose information unintentionally and unknowingly. Further, limiting disclosure to approved entities no longer functions to limit the likelihood of unauthorized access, re-disclosure, or repurposing. In focusing on disclosure, the statute does not account for the ways that student information might be used inappropriately by educational, as well as non-educational, actors.

Today's technology shatters these presumptions so that stakeholders no longer trust FERPA's institutional information management system. New shifts have disrupted information flow in the education ecosystem by creating new data collection, sharing, storage, application, and repurposing possibilities. Stakeholders can no longer be sure that FERPA adequately addresses their concerns. The following examination of the ways that new information practices alter the underlying mechanisms that made FERPA's delegation regime acceptable for so long highlights the most promising avenues for reform.

A. Unintentional and Unknowing Disclosure

Before student information was "datafied," educational actors oversaw almost all disclosure to outsiders, even under the information rules governing the School Official Exception. This was true of both paper and digital records. Unless someone accidentally left a file in the wrong place or a particularly determined outsider managed to access the school filing cabinet, sharing student information required intention.[176] It may have occurred in person—with school personnel relaying information to third parties or permitting them to review student files—over the phone, or by mail.[177] Disclosure to an outside party was a deliberate, periodic occurrence.[178] It necessarily involved the oversight and tacit approval of an educational actor—even under the informal rules governing the School Official Exception. Until recently, this was true of much digitized information as well, which often resided in dispersed, incompatible databases.[179]

FERPA's regulatory mechanisms rely on the assumption that it is not easy to share student records without individual or institutional action. Sharing student information was a periodic and predominantly intentional occurrence, generally involving conscious approval of the disclosure.

Today, sharing no longer requires conscious awareness, let alone approval. Data recipients frequently maintain their own student records subject only to virtual oversight.[180] Restricting disclosure to educational actors or approved recipients who use information to provide education-related services does not prevent them from repurposing data in ways that may not serve students' best interests.[181]

In a networked world, intention and knowledge are no longer required to disclose information, which frequently occurs continuously and automatically. Information may be disclosed accidentally through human or technological error, or involuntarily as the result of a deliberate hack. Further, "approved" disclosure in the absence of formal designation and documentation no longer implies that disclosure has been considered and sanctioned by educational institutions and agencies. As a result, a considerable amount of student

176. *See generally* RUSSELL SAGE REPORT, *supra* note 72.
177. *Id.*
178. *Id.*
179. *See* West, *supra* note 45, at 9.
180. *Id.*
181. *Id.*

information is shared pursuant only to the data recipient's vague terms of service and privacy policies.

B. Unauthorized Access and Virtual Oversight

When FERPA was enacted, the limited accessibility to physical records meant that most student data was not widely available or broadly repurposable.[182] The physical nature of student records created inherent buffers against unauthorized access and accidental disclosure and, accordingly, reduced the need for specific information governance and security protocols.[183]

It was also difficult to transfer and share digital student records until recently. They were not easily portable before cloud computing and typically required specific software to view and use their contents, resulting in siloed information dispersed in incompatible databases. The informal designation, constraints, and oversight regarding school official data recipients reflect and rely upon presumed confidentiality and educational use to benefit student data subjects.[184]

The boundary between insider and outsider blurs as educational institutions and agencies outsource many day-to-day functions to third parties. Student information is now also shared subject to a school's or district's virtual oversight.[185] Providing access to student records now implies sharing data that recipients are likely to retain on their own servers. Schools can only exercise virtual oversight over these records. As such, educational institutions are placed in the untenable position of overseeing third party practices in areas beyond their expertise.[186] Most schools have neither the ability nor time to oversee these records.[187] While the DOE guidance suggests

182. *See, e.g.*, FERPA 2008 DOE Analysis, *supra* note 112, at 6 ("Many districts and postsecondary institutions already use physical or technological controls to protect education records against unauthorized access, such as locks on filing cabinets for paper records . . . .").

183. *See id.*

184. *See generally* 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 (Marci Kanstoroom & Eric C. Osberg eds., 2008) (arguing that educators have an obligation to protect students' privacy).

185. Family Education Rights and Privacy, 73 Fed. Reg. 74816 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99) ("Exercising direct control could prove more challenging in some situations than in others.").

186. Molnar, *supra* note 117. Jim F. Siegl, a technology architect for the large Fairfax County district in Virginia, compares this to a regime that required new cars to drive fifty miles on one gallon, but required drivers to take the car apart to ensure compliance because gas mileage was not clearly indicated on window stickers. *Id.*

187. *Id.*

schools control "web-based and e-mail services" through "contract" provisions,[188] these are not required and, even when in place, frequently fail to cover basic aspects of information practices.[189]

C. Utility and the Ability to Repurpose

At the time of FERPA's enactment, student records were just beginning to expand beyond general administrative information like attendance and enrollment, summative assessment of student performance like end-of-semester grades, and, in some cases, teacher evaluation of behavior.[190] Information "generated" by students during day-to-day educational activities, such as class discussion and answering questions, could not be captured in any detail. FERPA sought to reinforce existing norms so that student data would remain in the immediate education environment.[191]

With respect to outside actors, the statute sought to regulate government, not private, record-keeping.[192] The School Official Exception was intended to apply to actors who primarily used information within or at the direction of an educational institution.[193] The content of student records was primarily useful as a means to evaluate a specific student. There were few other ways to employ, let alone repurpose, student information. As one scholar notes, most of the "use" contemplated by FERPA at the time of its enactment was, "in reality, a type of disclosure of a record."[194] As a result, limiting

188. Family Education Rights and Privacy, 73 Fed. Reg. 74816. For example, the DOE suggests that schools outsourcing information technology services use contract provisions to restrict third parties from using or allowing access to PII from education records "except in accordance with the requirements established by the educational agency or institution that discloses the information." *Id.*

189. CLIP STUDY, *supra* note 36, at 29.

190. *See Divoky, supra* note 71, at 14 (expressing concerns about student records that include not just "hard data, such as IQ scores, medical records, and grades," but also "soft data," such as teacher anecdotes, notes on parent interviews, and disciplinary reports that are "routinely filed away in school offices or stored in computer data banks").

191. *Study Session Regarding inBloom, Inc., Before the Colo. State Bd. of Educ.*, EPIC.ORG 4 (2013) (Testimony and Statement for the Record of Khaliah Barnes), https://epic.org/privacy/student/EPIC-Stmnt-CO-Study-5-13.pdf.

192. 34 C.F.R. § 99.1.

193. 120 CONG. REC. 13,952 (1974) (preceding FERPA's passage, Buckley stated "[i]n the wake of recent scandals over Government spying and secrecy, President Nixon announced the establishment of a high-level committee to provide a 'personal shield for every American' against all invasions of privacy. Surely we must not exclude our children from this protection."); *see also* Penrose, *supra* note 155 at 83–84.

194. Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public School Children*, 84 NEB. L. REV. 1158, 1203 (2006).

disclosure to approved actors also served to limit the degree to which it could be used toward non-educational purposes.[195]

FERPA did not anticipate a world in which information could be put to endless purposes by educational and non-educational entities. Today, the identity of an education-related actor or presence of a legitimate educational interest does not prevent an educational institution, agency, or data recipient from repurposing information to serve secondary interests beyond the immediate provision of education services. Regulating disclosure no longer ensures appropriate information use by either educational actors or data recipients, as these entities can put information obtained in the course of providing services to educational institutions and agencies that facilitate the provision of education, to secondary purposes.

IV. THE FLAWS OF FIPPS-BASED STUDENT PRIVACY/FERPA REFORM

Without the barriers of physical limitations, presumed education-related purpose, and non-profit motives, stakeholders no longer trust FERPA's informal delegation framework. Privacy advocates and stakeholders seek regulation of entities receiving information from educational institutions, and more specific constraints on substantive data practices regarding the collection, use, retention, governance, and security of student information.

Stakeholders want more control over the data practices of educational institutions and agencies as well as third-party data recipients.[196] This includes narrowing the type and quantity of infor-

195. In addition, FERPA's focus on anonymization may no longer protect against the type of hidden and decontextualized decision-making Buckley sought to preempt. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010). However, broader discussion of identifiable issues is outside the scope of this Article.

196. *See, e.g.*, Herold, *Americans Worried*, *supra* note 58; Davis & Cavanagh, *supra* note 58; Roscorla, *supra* note 58; Barnes, *supra* note 58; *Common Sense Media*, *supra* note 43; Simon, *Big Biz*, *supra* note 43; Singer, *supra* note 58; John Podesta, *Big Data and Privacy: 1 Year Out*, WHITE HOUSE (Feb. 5, 2015, 9:29 AM), http://www.whitehouse.gov/blog/2015/02/05/big-data-and-privacy-1-year-out ("As more data is collected, analyzed, and stored on both public and private systems, we must be vigilant in ensuring the balance of power is retained between government and citizens and between businesses and consumers."); Diane Ravitch, *How to Protect Student Privacy*, DIANE RAVITCH'S BLOG (Jan. 14, 2015), http://dianeravitch.net/2015/01/14/how-to-protect-student-privacy [hereinafter Ravitch, *How to Protect*]; Barnes & Strauss, *supra* note 2.

mation collected about students,[197] how long it can be stored,[198] and how it is protected against unauthorized access.[199] They demand more formal procedures and record-keeping of data-related decsion-making and flow. They want educational institutions and agencies to document the purpose of collection and the security measures implemented for every collection and use of data, so parents and students can access information held by third parties, and that they impose security requirements to prevent unauthorized access.[200]

Stakeholders also want to bar educational institutions and agencies from disclosing data to particular entities, using the data in certain ways, and repurposing the data, or else, in the alternative, require parental or student consent before any such action.[201] They are particularly concerned about entities that provide services like applications, information management, and instructional content to educational institutions using student information for commercial or marketing purposes.[202] They want direct accountability mechanisms to encourage strict compliance and redress potential injuries resulting from inappropriate information practices.[203]

197. Barnes & Strauss, *supra* note 2; Ravitch, *How to Protect*, *supra* note 200; *see* STUDENT DATA PRINCIPLES (2014), http://studentdataprinciples.org/wp-content/uploads/2015/03/Student-Data-Principles-FINAL.pdf.

198. Edward J. Markey & Orrin Hatch, *Protecting Student Privacy in the Digital Age*, THE HILL (May 15, 2015, 6:00 AM), http://thehill.com/opinion/op-ed/241997-protecting-student-privacy-in-the-digital-age.

199. Natasha Singer, *Schools Use Web Tools, and Data Is Seen at Risk*, N.Y. TIMES (Dec. 12, 2013), http://www.nytimes.com/2013/12/13/education/schools-use-web-tools-and-data-is-seen-at-risk.html; STATE STUDENT DATA PRIVACY LEGISLATION, *supra* note 3.

200. *See* Barnes & Strauss, *supra* note 2; Markey & Hatch, *supra* note 202; Ravitch, *How to Protect*, *supra* note 200; STUDENT DATA PRINCIPLES, *supra* note 201.

201. Press Release, U.S. Senator David Vitter, *Vitter Introduces Student Privacy Protection Act*, VITTER (May 14, 2015) [hereinafter Vitter], *available at* http://www.vitter.senate.gov/newsroom/press/vitter-introduces-student-privacy-protection-act ("We need to make sure that parents and students have complete control over their own information.").

202. *See, e.g.*, Markey & Hatch, *supra* note 202; Ravitch, *How to Protect*, *supra* note 200; CLIP STUDY, *supra* note 36; Podesta, *supra* note 200 ("[A]s technologies proliferate in the classroom, we must be vigilant about ensuring that students' privacy is protected in the educational context and that their education data is not mined for commercial or marketing purposes.").

203. *See, e.g.*, Vitter, *supra* note 205 (imposing monetary fines on educational actors for noncompliance); Press Release, Comm. On Educ. & the Workforce, Rokita, Fudge Introduce Bipartisan Bill to Update Student Privacy Protection (July 22, 2015) [hereinafter Rokita], *available at* http://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=399178 (seeking to "clarif[y] the definition of student records and how they are kept, increase[ ] parental access and consent, strengthen[ ] accountability and transparency, and protect[ ] student records from dangerous data breaches and theft").

A. Regulatory Responses

Legislators, advocates, and industry groups have responded to stakeholder concerns by proposing a flurry of reform proposals and guidelines. As of July 2, 2015, "forty-six states considered 182 bills addressing student data privacy" and twelve passed twenty-four new laws.[204] On the federal level, Congress has introduced five student privacy bills. Bills proposed by Senators Edward J. Markey and Orrin Hatch, Senator David Vitter, and Representatives Todd Rokita and Marcia Fudge could amend FERPA.[205] Two other bills, sponsored by Representative Messer and Senator Blumenthal, respectively, propose to regulate entities that receive information from educational institutions and agencies.[206] Many companies in the education technology industry have also pledged to adhere to certain information practices through Student Privacy Pledge, organized by the Future of Privacy Forum and the Software & Information Industry Association (SIIA).[207]

B. Regulating Educational Actors Through FERPA Amendments

The FERPA reform proposals rely on several different regulatory mechanisms to accomplish these aims. Most protect a broader array of information.[208] Many bolster FIPPs-based privacy protection by increasing transparency and notice, giving parents and students more opportunities to exercise individual control over information, and ensuring more comprehensive access to student information. Several require schools to maintain adequate security to prevent unauthorized access.[209]

The proposed amendments go beyond FERPA's focus on disclosure to impose constraints on school collection, use, retention, and

---

204. Rachel Anderson, *EdData Privacy Update: 7/2/2015*, DATA QUALITY CAMPAIGN (July 2, 2015), http://dataqualitycampaign.org/blog/2015/07/eddata-privacy-update-722015.

205. Protecting Students' Privacy Act of 2015, S. 1322, 114th Cong. (2015); Student Privacy Protection Act, H.R. 3157, 114th Cong. (2015).

206. Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092, 114th Cong. (2015); SAFE KIDS Act, S. 1788, 114th Cong. (2015).

207. *About the Student Privacy Pledge*, PLEDGE TO PARENTS & STUDENTS, http://studentprivacypledge.org/ (last visited Apr. 18, 2016).

208. *See, e.g.*, Rokita, *supra* note 207 ("Updates the definition of an education record to ensure student information connected to classroom technology is protected."). This expansion is important to provide more comprehensive protection for potentially sensitive student information, such as metadata, that are not addressed in the current federal regulatory regime, but further analysis of these provision is beyond the scope of this Article. *Id.*

209. *See, e.g.*, *id.* (discussing "strengthen[ing] security requirements for storing and gaining access to student education records").

repurposing requirements. They also restrict on particular information practices, with a focus on preventing student data from being sold or used to drive targeted advertising. Several reform proposals would impose direct liability on educational actors as well through fines or a private right of action.[210]

The FERPA amendments also attempt to regulate outside service providers indirectly by imposing more requirements that must be met for third parties to qualify as appropriate data recipients.[211] Some require private agreements between the parties by having them stipulate to joint liability and include penalties for security breaches in violation of the agreements.[212]

These proposals display vastly different assessments of the normative propriety of various information practices like using student information for research or product development. While a detailed evaluation of specific reform provisions is beyond the scope of this Article, analyzing these proposals in terms of the framework set out above helps reveal whether they will adequately address stakeholder concerns.[213]

---

210. *See, e.g.*, S. 1341 § 5.

211. *Id.* § 3.

212. *See id.* § 3, 10–11; H.R. 3157, 114th Cong. § 5, 11 (2015).

213. The Markey-Hatch amendment most closely resembles FERPA's current regulatory structure and compliance-oriented enforcement. It adds more requirements before educational actors can disclose information that are designed to ensure that data recipients hold covered information securely, provide parents and students with access to the information, and do not use the information to advertise or market a product. S. 1322, 114th Cong. (2015).

The Vitter Bill is an aggressive attempt to curb educational actors' discretion over procedural and substantive information practices. It focuses on providing parents and students with more control over information. It also imposes substantive prohibition on various information practices, including a ban on collecting data about a variety of student characteristics, marketing and advertising to students based on covered information, and using data for delving or improving products or services and psychological testing. S. 1341 § 6. The Bill creates a private right of action for noncompliance and proposes significant fines for FERPA violations on a per student basis. *Id.* at 5.

The Rokita-Fudge proposal ensures more FIPPs with better record-keeping by educational institutions and agencies and imposes requirements that a data recipient must stipulate to in written agreements. It provides parents and students with more opportunities to exercise consent over disclosure and complete discretion to opt out of data use for research, even by educational actors. It allows parents and students to exercise consent over educational institution and agency disclosure, except for directory information, relevant education processes, and recipients who have stipulated in written agreements to transparency, record-keeping, access, security, and re-disclosure requirements. It also imposes fines for FERPA violations, but, consistent with FERPA's current model, only after attempts to bring educational entities into compliance. 20 U.S.C. § 1232g(b)(7)(B)(f) (West 2013) ("[A]ction to terminate assistance may be taken only if the Secretary finds there has been a failure to comply with this section, and [the Secretary] has determined that compliance cannot be secured by voluntary means.").

Much of the debate surrounding these reform proposals focuses on their specific requirements. It does so at the expense of accounting for FERPA's delegation-based regulatory structure and the specific considerations of the education context. Without taking these into account, many of the proposed reforms will not achieve the aims of stakeholders and policymakers, regardless of the normative propriety of their substantive requirements.[214]

C. Flawed FIPPs-Based Reform Mechanisms

Many policymakers have responded by trying to create more transparency and shift control over information practices back to parents and students. Reform proposals seek to bolster FERPA's alignment with the FIPPs by providing more opportunities for consent, more detailed transparency, and expanded access to student information. In an article setting out a Student's Bill of Rights, a privacy advocate said, "We need to put students back in control of their data, the way FERPA . . . imagined."[215]

All of the proposed reform measures would increase transparency of practices regarding student information.[216] A common approach for current reform is to enlarge the circumstances under which parents and students can exercise consent over disclosure and add additional opportunities for privacy self-management with respect to information use and repurposing practices. The proposed reforms require more specific information in notices used to obtain parental or student consent, including the data shared, reasons for disclosure, and recipients.[217] Some require consent for certain information practices like using covered information to conduct research.[218]

---

214. H.R. 3157 § 4.

215. Barnes & Strauss, *supra* note 2.

216. For example, the Rokita-Fudge Bill requires public posting about the types of data collected about students, the actors with whom this information is shared, the purposes served by this collection and disclosure, and the security measures in place. H.R. 3157 § 5. Both the Markey-Hatch Bill and the Rokita-Fudge Bill add record-keeping requirements regarding data recipients. *Id.* § 4; S. 1322 § 2. The Rokita-Fudge Bill, for example, requires educational institutions and agencies to keep records about the individuals, agencies, or organizations that request or obtain access to a student's education records. H.R. 3157 § 4. It also requires educational institutions and agencies to enter into a written agreement before sharing information and to designate an official to maintain data security. *Id.*

217. The Rokita-Fudge Bill requires the notice included with written consent to disclosure forms to include information specifying the applicable records, reasons for their disclosure, data recipients, and, upon request, a copy of the shared records. H.R. 3157 § 5.

218. The Vitter Bill, for example, requires parental consent before educational institutions and agencies can share "data of students, including personally identifiable information and directory information" with third parties, including school officials, regardless of FERPA's ex-

While intuitively appealing, heavy reliance on consent provisions will not create the oversight or control over information practices that stakeholders seek. As many scholars have noted, FIPPs-based privacy regimes rarely provide meaningful individual control *over* information or protection against inappropriate data flow.[219] Notice and consent models rarely result in informed, voluntary user acceptance.[220] Notice is either too complex to comprehend or too vague to provide an adequate sense of data recipients' information practices.[221] The sheer quantity of data recipients and constantly changing policies make the consideration of terms of use and privacy policies impossibly time consuming.[222] Scholars discuss how consent cannot be considered voluntary given the take-it-or-leave-it nature of click-wrap privacy policies, the lack of readily available and low-cost alternatives, and prohibitively high costs of opting out.[223] Furthermore, human psychology and institutional and economic structures skew user decision-making in favor of acquiescing to unexamined information and privacy policies.[224]

In most cases, uninformed or insignificant FIPPs-based privacy regimes provide data recipients with tremendous leeway over how they handle and use their user information. In many circumstances, consent options will default to institutional decision-making. This creates an illusion of control over student information practices, and, without additional substantive constraints, gives educational actors broad discretion based on token consent. Accordingly, con-

---

isting exceptions. S. 1341 § 3. The Rokita-Fudge Bill also requires consent before educational institutions and agencies can disclose information to third parties who "advertise or market a product or service . . . or . . . for the development of commercial products or services." H.R. 3157 § 9. It permits parents and students to opt out of research using students' data, even if educational institutions or agencies conduct such research. *Id.* § 5.

219. *See, e.g.*, Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 273–74 (2012); *see also* Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data*, 3 INT'L DATA PRIVACY L. 3, 4 (2013).

220. Cranor, *supra* note 223, at 274; *see also* Cate & Mayer-Schönberger, *supra* note 223.

221. *Id.*

222. *See, e.g.*, Norman Sadeh et al., *The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About*, CARNEGIE MELLON U. (Dec. 2013), http://reports-archive.adm.cs.cmu.edu/anon/isr2013/CMU-ISR-13-119.pdf.

223. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS J. AM. ACAD. ARTS & SCI. 32, 35 (2011).

224. *See, e.g.*, Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 512–13 (2015).

sent-based privacy protection may result in less, not more, oversight and protection against inappropriate data use.[225]

Very detailed and comprehensive notice is also questionable in actually providing parents and students with information upon which to base a decision. As in other spheres, notice provisions become so detailed that they overwhelm users or so broad as to provide little meaningful content about specific information practices.[226] The same is true with respect to FERPA's access provisions. The wealth and complexity of data collected about students undermines the efficacy of using parent and student oversight as a means to ensure information accuracy.[227] Parents typically do not have the necessary expertise or time to examine each potential primary and secondary use of a student's data or the capacity to evaluate potential data recipients.

D. Problematic Privacy Self-Management

The theory underpinning of FIPPs' "informed consent" is also more suspect in the education context. Even with adequate and comprehensible notice, parent or student consent in an accredited education system does not reflect a voluntary choice among realistic alternatives.[228] Compulsory attendance at education institutions makes the concept of "choice" illusory. Stakeholders who disagree with school information practices could theoretically satisfy this requirement through homeschooling or enrollment in a private institution that has more acceptable information practices. For most stakeholders, however, these options are neither practical nor affordable alternatives to the public education system.[229] While attend-

225. *See generally*, Symposium, *Disclosure and Notice Practices in Private Data Collection*, 32 CARDOZO ARTS & ENT. L.J. 784 (2014) (discussing different methods of privacy notices).

226. Ellis Booker, *Education Data: Privacy Backlash Begins*, INFORMATIONWEEK (Apr. 26, 2013, 9:35 AM), http://www.informationweek.com/education-data-privacy-backlash-begins/d/d-id/1109713 ("The complexity and sophistication of the data uses would make it difficult for the average parent to know what they're consenting to." (quoting interview by Ellis Booker, Journalist, InformationWeek, with Joel Reidenberg, Law Professor, Fordham University School of Law)).

227. The practicality of this provision has been challenged by the proliferation of data and different data systems. In response to a recent request by a Nevada parent to review his child's records, the Nevada Board of Education indicated that it could not fulfill the request because doing so would require the acquisition of $10,000 worth of technology. Herold, *$10,000 Price Tag*, *supra* note 89.

228. *See* Martin C. McWilliams, *Applicants Laid Bare: The Privacy Economics of University Application Files*, 34 HOFSTRA L. REV. 185, 190 (2005).

229. Joseph Jerome, *Buying and Selling Privacy Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 50–52 (2013), http://www.stanfordlawreview.org/online/privacy-

ing a higher education institution is not required, the socioeconomic value placed on obtaining an advanced degree is sufficiently strong as to be coercive, and almost certainly outweighs concerns about information practices.[230]

Even if educational institutions could implement measures to ensure that parents and students could make informed, meaningful choices among realistic alternatives, privacy self-management in the education context may not be possible, or normatively desirable, due to practical, political, pedagogical, and philosophical reasons.[231]

1. Practical obstacles

On a practical level, considering individual privacy preferences would overwhelm educators and administrators.[232] The process of providing notice and obtaining consent would in itself be tremendously burdensome.[233] Former Secretary of Education Arne Duncan has stated:

> FERPA allows disclosure without consent because there are essential and legitimate educational needs to disclose data where parental control cannot be reasonably implemented. Obtaining consent is not feasible in some instances, such as when a school district is disclosing PII from education records on its students to a contractor to operate the district's student records system.[234]

2. Political authority

Politically, the American system allocates authority among state and local, not federal, educational entities.[235] FERPA's delegation model accommodates this highly heterogeneous and "radically decentralized" education system.[236] Educational institutions vary tre-

---

and-big-data/buying-and-selling-privacy (discussing the pressures on the poor to trade data for services).

230. *See, e.g.*, JEFFREY J. SELINGO, COLLEGE UNBOUND: THE FUTURE OF HIGHER EDUCATION AND WHAT IT MEANS FOR STUDENTS 5–12 (2013) (discussing the "tyranny of the degree").

231. Jules Polonetsky & Joseph Jerome, *Student Data: Trust, Transparency, and the Role of Consent*, FUTURE OF PRIVACY FORUM 7-11 (Oct. 2014), http://www.futureofprivacy.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf.

232. *Id.* at 7.

233. *Id.*

234. Duncan, *supra* note 92, at 3.

235. *See* David F. Labaree, *Public Goods, Private Goods: The American Struggle over Educational Goals*, 34 AM. EDUC. RES. J. 39, 59 (1997).

236. *Id.* at 59.

mendously in terms of resources, technological sophistication, and normative assessment of data-driven education tools.[237] FERPA accommodates this diversity by deferring to education decision-makers. Secretary Duncan has noted that FERPA's "regulations do not require a 'one-size-fits-all' approach . . . because we recognize that each school or school district needs to develop its own policies and procedures to meet its individual needs."[238] This accommodates schools with different resources, technological sophistication, and views about the normative propriety of various information practices.[239]

3. Pedagogical considerations

In importing regulatory regimes from other contexts, policymakers seeking to protect student privacy must consider the importance of information practices on pedagogy. This requires a different framework and expertise than regulating more standard and static commercial exchanges.

Regulating privacy regarding the online sale of a widget or transfer of financial or medical information is qualitatively different than transferring information in education because altering information practices in education alters education itself. The privacy practices of sellers, buyers, and digital intermediaries will not alter the utility of the widget purchased online or medical information transferred to a new doctor. Even tracking readers on e-books (without adding supplemental features) does not alter the content of the book itself. Regulating information exchange in education, however, regulates the "content" of the education itself. In altering the conditions and scope of this exchange, rules governing student data may have profound pedagogical effects.

4. Philosophical goals

Philosophically, there may be normative reasons for prioritizing institutional, over individual, decision-making.[240] A system based on privacy self-management does not account for broader social and

237. Plunkett, Solow-Niederman & Gasser, *supra* note 21, at 5–7.

238. Duncan, *supra* note 92, at 7–8.

239. *See* Plunkett, Solow-Niederman & Gasser, *supra* note 21, at 5–7; *see generally* MEISTER & SOLOW-NIEDERMAN, *supra* note 42, at 5–6.

240. Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 169–71 (2010).

context-specific consequences.[241] Consideration of these consequences is crucial in education, which is traditionally considered a public good.[242] As technology becomes increasingly central to classroom education, educational institutions will struggle to provide equivalent instruction and education to students who opt out of mainstream information practices.[243] Even in cases where parents and students can exercise choice over information practices, it may be impossible for schools to provide equivalent experiences to students who opt out of mainstream instructional practices.[244] It might increase the "digital divide" by impeding teachers from providing equivalent education to students in the same classroom who cannot use the same technological tools.[245]

V. MOVING BEYOND FERPA AND FIPPS

Additional reform should address the upset of information norms that made FERPA's delegation model acceptable for almost forty years. As discussed above, FERPA has existed alongside practical and technological limitations that provided: practical obscurity and security against unauthorized and involuntary disclosure; confidentiality and educational use serving student or institutional interests;

---

241. *Id.*; *see also* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent, in* PROCEEDINGS OF THE ENGAGING DATA FORUM: THE FIRST INTERNATIONAL FORUM ON THE APPLICATION AND MANAGEMENT OF PERSONAL ELECTRONIC INFORMATION (2009); Polonetsky & Jerome, *supra* note 235, at 9 ("Opt-outs may bias or otherwise limit the sample sizes needed to plot a course forward, effectively compromising the ability of state and local officials to accurately measure education outcomes. When a significant portion of students are missing from a sample, any results would be skewed. This [shortfall] affects the ability to accurately evaluate educational programs, and potentially impacts the distribution of federal education grants and services, further hurting those schools and students most in need."); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. Rev. 1880, 1886 (2013).

242. Taxpayers support most educational entities, either through direct federal funding or student loans. Roy Y. Chan, *Higher Education and the Public Good: A Critical Historical Analysis from the Colonial Period to the Golden Age Era* (Oct. 2, 2012), *available at* http://rychan.com/doc/Higher_Education_and_the_Public_Good.pdf.

243. *See* Polonetsky & Jerome, *supra* note 235, at 8–10; *see also* Gene Sperling, *Bridging the Digital Divide, From the Front Lines*, WASH. POST (Nov. 13, 2013), http://www.washingtonpost.com/postlive/bridging-the-digital-divide-from-the-front-lines/2013/11/12/95c14966-4b28-11e3-be6b-d3d28122e6d4_story.html.

244. *See* Sperling, *supra* note 247*; see also* Robert Kolker, *The Opt-Outers*, N.Y. MAG. (Nov. 24, 2013), http://nymag.com/news/features/anti-testing-2013-12/index4.html (quoting the New York State deputy education commissioner, cautioning parents "that if they remove their child from the assessment program, there's an impact. We really believe that these tests are not only important but irreplaceable. A parent who opts out of that is giving up the opportunity to get a critical piece of information.").

245. *See* Sperling, *supra* note 247.

and intentional disclosure and immediate oversight of data recipient information practices.

This Article has presented the difficulties of providing meaningful notice and consent mechanisms, as well as the potentially problematic consequences of relying on privacy self-management in the education context. Instead, reform efforts should focus on providing new regulatory mechanisms that provide meaningful constraints in lieu of physical protection and FIPPs-based notice, consent, and authorization. These reforms should reassure stakeholders that individuals and entities with access to student information would process it securely, keep the scope of disclosure contained, and use the information to serve educational interests.

While requiring better transparency, formalized disclosure mechanisms, and more specific criteria regarding appropriate data security, use, and retention will ameliorate some of FERPA's flaws, contemporary privacy concerns would be better addressed through new, separate measures. The flexibility of FERPA's delegation-based regulatory regime accommodates the diversity of educational institutions, but does not provide sufficient assurance to stakeholders in light of new information technology and practices. The Department of Education has valiantly attempted to shoehorn a forty-year-old statute to match today's information systems, but the statute has been stretched to its limits.

A better approach accounts for the fact that FERPA's regulatory structure is a poor way to provide significant control over institutions' information practices or impose direct consequences for privacy violations. However, reforms that permit institutional discretion will only succeed if there is sufficient trust in the reforms' data-related decision-making. This shift requires meaningful transparency, public oversight, and accountability. Indeed, to ensure public accountability, institutional decision-making must be accompanied by significant transparency and oversight. Finally, FERPA provides a poor tool to indirectly control non-educational actors. Rather than requiring individuals or educational institutions to oversee data recipients—an ineffectual practice that overburdens those who abide by it—reform should apply directly to problematic actors or practices, whether through formal or voluntary mechanisms.

A. Procedural Regulation of Education Entities

The reform proposals all seek to refine the requirements within FERPA's delegation framework. They increase transparency about information practices regarding student information. They impose

procedural and governance requirements to provide more documentation of data flow, requiring schools to have a comprehensive inventory of their information ecosystems. Several reform principles also prompt more deliberate decision-making regarding information disclosure by requiring schools to promulgate more specific security and privacy protocols and articulate the educational interest served by data disclosure.

Broadening the scope of information protected, creating more governance, and requiring more documentation and deliberate data-related decision-making can certainly improve FERPA's privacy protections. Proposed procedural requirements can fill crucial gaps in FERPA's current framework, particularly with respect to informal and undocumented decision-making under the School Official Exception. Allowing educational actors to exercise discretion regarding information practices with a wide range of acceptable options will accommodate the diversity of actors in the education system, emerging privacy norms, and ever-changing technologies. Transparency requirements are not sufficient, but will at least promote public oversight of the ways schools exercise discretion over student data. However, reforms that impose extra procedural requirements and also allow for significant discretion over data-related decisions will only be successful where transparency and documentation allow stakeholders and policymakers to oversee and review decisions.

B. Substantive Regulation of Education Entities

Unlike FERPA's current incarnation, today's reforms seek to regulate educational actors' collection, use, storage, and retention of student information. Many of these reforms impose oversight and security requirements, limit data collection, and impose substantive constraints on specific information uses, actors, and purposes served, particularly selling student data or using it for targeted marketing and advertising.

Substantive constraints will be necessary to ensure specific control over unacceptable student information practices in the absence of effective privacy self-management. These constraints could include data minimization and limited retention requirements, use/repurposing restrictions, and technological due process mechanisms[246] that take the values and purposes of the education context

246. *See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1301–13 (2008) (discussing technological due process); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 124–28 (2014) (discussing "predictive privacy harms" and advocating for the implementation

into account.[247] Measures such as these would ensure baseline student privacy protection, without relying on ineffectual notice and consent mechanisms or institutional discretion.

The difficulty lies in ensuring that these measures have the proper scope and specificity. With such a diverse array of stakeholders and educational institutions, strict rules are likely to be either too broad to provide meaningful constraint over information, or too rigid to accommodate varied and constantly changing viewpoints and technologies. Accordingly, substantive constraints will work best to create baseline privacy protections with broad consensus or prevent particularly egregious information practices.

C. Accountability and Liability

Educational actors have tremendous incentive to comply with substantive requirements to the best of their ability. At the same time, FERPA's compliance-orientation accommodates a fair degree of accidental, unavoidable, or unknowing noncompliance without imposing any consequences. As today's student privacy debate shows, simply imposing requirements on educational actors is not enough to assuage stakeholders without sufficient transparency and accountability. Many proposed reforms recognize this need and suggest varied enforcement mechanisms more directly targeted than "policies and practices" and less drastic than withdrawal of federal funds.[248] Imposing liability based on FERPA violations or resulting harm to students, rather than an institution's policy or practice of noncompliance, fundamentally shifts FERPA's regulatory mechanism.

On a symbolic level, the impact is immense since both educational institutions and data recipients have significant financial incentives to ensure compliance. At a practical level, however, it is unclear

---

of a procedural due process framework in the private sector); Solon Barocas, Sophie Hood & Malte Ziewitz, *Governing Algorithms: A Provocation Piece*, 1, 8–9 (Mar. 29, 2013) (unpublished), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2245322 (discussing the use of algorithms in data collection, due process, and rule-making).

247. *See* Polonetsky & Jerome, *supra* note 235, at 9. The propriety of these practices depends in large part on what one views as the purpose of education in America. *See* Barocas & Nissenbaum, *supra* note 245.

248. While the Markey-Hatch Bill relies on FERPA's existing enforcement mechanisms, the Vitter and Rokita-Fudge Bills impose direct financial consequences for educational actors who violate FERPA. The Vitter Bill creates a private right of action for FERPA violations. S. 1341, 114th Cong. § 5 (2015). Students and families could recover at least $1,000 per child for the first offense, at least $5,000 per child for the second offense, and at least $10,000 per child for the third offense. *Id.* An early draft of the Rokita-Fudge Bill creates direct liability for FERPA violations that cause harm to students, with fines of $2,000 per student harmed up to a maximum of $500,000. (On file with author.)

whether educational institutions and third parties will actually be held accountable for noncompliance, and whether enforcement will be so detrimental to institutions that it harms students and undermines the broader goals of the education context in the process.

Creating strict liability for noncompliance, as several reforms do, may create more accountability, but may do so at the cost of the broader mission—educating students—by depriving educational institutions and agencies of already scant resources, harming students in the process. Similarly, permitting parents and students a private right of action, in and of itself, would create an unmanageable volume of actions that educational entities would have to defend against.

FERPA's compliance-orientation recognizes that no privacy system is perfect, and that schools will inevitably violate imposed constraints. It provides them room to do so without imposing strict liability and severe penalties that would ultimately hurt the very students the statute seeks to protect. Accountability measures must be sufficiently lenient to accommodate unpredictable and unpreventable privacy violations that will occur even in the absence of nefarious intent or gross negligence. Safe harbors and similar mechanisms should be explored to determine the best means to balance accountability and flexibility. A co-regulatory regime is also a promising alternative to the binary, and frequently unsatisfying, choice between rigid and slow public action and the potential laxity of self-regulation.[249]

D. Indirect Regulation of Data Recipients

The proposed reforms also seek to regulate data recipients indirectly by imposing requirements that must be met for third parties

249. An enforcement structure modeled after the Children Online Privacy Protection Act (COPPA), for example, would combine the flexibility of self-regulation with the accountability provided by FTC approval of a limited number of safe harbors. This enforcement method avoids the proliferation of independent and unique systems that are unmanageable at scale. It also outsources auditing to third parties and the FTC instead of putting the burden of audits on the small number of Department of Education employees. Limiting the number of configurations not only permits more comprehensible transparency regarding core data policies and protections offered by various entities, but also encourages marketplace competition to provide various levels of constraint on information flow. *See, e.g.*, Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J. L. & POL. INFO. SOC'Y 355 (2011); *see also* Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE BY THE U.S. DEPARTMENT OF COMMERCE (1997).

to qualify as appropriate data recipients.[250] These frequently include conditions that the data recipient not sell student information or use it to drive targeted marketing.[251] Some do so by imposing additional requirements that data recipients must satisfy to receive information from educational actors under the School Official Exception. Others adopt the model created by the 2008 and 2011 amendments to FERPA's studies and audit and evaluation exceptions. They would similarly require recipients to stipulate to specific practices in written agreements governing the disclosure of information.[252]

FERPA is an improper tool to regulate the practices of (suspect) entities using sensitive student information. Indirect regulation of data recipients will suffer the same limitations as FERPA's existing oversight requirements that fail to provide sufficient oversight and accountability to address stakeholders' concerns.[253] Under proposed reforms, educational institutions are tasked with knowing and evaluating outside parties' security, disclosure, and retention practices, as well as those of subcontractors or advertisers with whom they share student data in the course of providing their services. This includes inquiring about data recipients' protocols regarding encryption in data transfer and storage, differential access to student data for internal actors or subcontractors based on responsibility, and segregation of personally identifying data from other information.

These practices would require educational entities to determine whether the third party data processing would be considered

250. *See generally* S. 1322, 114th Cong. (2015). The Markey-Hatch Bill seeks to regulate the information practices of outside parties. *Id.* § 4. The Rokita-Fudge Bill seeks to govern "education service provider[s]," defined as "any provider, other than a school official or employee, of services developed and targeted to students for an educational purpose, whether specifically marketed to schools, institutions of higher education, educational agency or institution employees or officers, or other individuals primarily engaged in the provision of education services." H.R. 3157 § 15(5).

251. The Markey-Hatch Bill, for example, restricts schools from knowingly sharing information with third parties who will use it for advertising and marketing purposes. S. 1322 § 2. Similarly, the Rokita-Fudge Bill prohibits schools from entering into contracts—that the statute requires to authorize disclosure of student information—with an "education service provider" that has a "policy or practice of using, releasing, or otherwise providing access to personally identifiable information to advertise or market a product or service; or for the development of commercial products or services" without parental consent. H.R. 3157 § 9.

252. S. 1322 § 2.

253. Leslie Gallagher Moylan, *Pass or Fail? Sens. Markey and Hatch Introduce "Protecting Student Privacy Act" Seeking to Amend FERPA, Increase Protection of Student PII Shared with Private Companies*, JD SUPRA BUS. ADVISOR (Aug. 6, 2014), http://www.jdsupra.com/legalnews/pass-or-fail-sens-markey-and-hatch-int-44799; *see* Leslie Gallagher Moylan, *"A" for Effort? Senator Markey Announces Latest Privacy Legislation Aimed at Protecting Student Data*, JD SUPRA BUS. ADVISOR (Jan. 17, 2014), http://www.jdsupra.com/legalnews/a-for-effort-senator-markey-announces-63241.

maintenance,[254] or prohibited "development."[255] Proposed reforms would require schools to keep up with any adjustments to platforms or content that relates to the provision of services, and to decipher how essential these data users are to the provision of services to these schools in the future.[256] All of the data-driven applications used by the institution and its employees—a number well into the hundreds for most institutions—would require close attention. Additionally, FERPA's enforcement mechanisms do not apply to entities that do not receive federal funding, and attempting to regulate data recipients indirectly will be both costly and ineffective.

The use of contracts to impose requirements reduces educators' burden of oversight under the assumption that data recipients comply with their provisions. Contracts provide more flexibility than broad regulations in accounting for differences between institutional needs and technological change than statutory provisions. Even with contractually imposed information practices, however, educational actors will still bear the burden of investigation and oversight, and potentially crippling liability. They would still have to conduct due diligence before entering into agreements with data recipients, and would need to monitor data recipient practices to ensure continued compliance with the terms of the agreement. Schools may not have the resources, market power, or technological and legal sophistication to evaluate, consider, and impose terms on data recipients.

Further, requiring contracts for all disclosures ignores the complexity of day-to-day information flow in education institutions. The state education agencies governed by the studies, audit, and evaluation exceptions, and the higher education institutions using the studies exception already vet queries regarding research projects and contractors. The audit and evaluation exception generally involves periodic disclosures by state education agencies to contractors creating large-scale data systems.[257] These multi-million dollar

254. H.R. 3157 § 5.

255. *Id.* §§ 5, 9 (prohibiting educational institutions and agencies from contracting to disclose information to recipients who uses PII data for "the development of commercial products or services").

256. *See id.* § 9. Under the Markey-Hatch Bill, for example, educational entities would be responsible for evaluating the data recipient's access capabilities to confirm that parents and students would have the same access rights provided under FERPA as they would with respect to educational institutions. S. 1322 § 2. Additionally, the educational entities would have to ensure that the recipients use appropriate security protocols. *Id.* The Rokita-Fudge Bill also requires educational institutions and agencies to ensure that data recipients have security and access protocols in place that, at a minimum, match or exceed "the commonly accepted industry standards on privacy protection." H.R. 3157 § 5.

257. *See* 34 C.F.R. § 99.35(a) (2012).

systems are limited in number and their disclosure of student information is subject to considerable legal oversight and contract negotiation..[258] Disclosure of student information governed only by terms of service and privacy policies will not be subject to similar, if any, overview to ensure appropriate data practices.

The reform proposals also use FERPA to impose liability on data recipients.[259] Some rely on contractual provisions to provide means for redress through breach of contract claims, stipulated penalties, or assumption of joint liability.[260] Enforcement would also require educational institutions and agencies to be involved in suits that might require considerable resources with no guarantee of a favorable outcome.

One proposal suggests that violations by parties who are not subject to Department of Education enforcement be reported to the Federal Trade Commission or the Attorney General for further action.[261] This system would at least hold data recipients accountable for FERPA noncompliance. It creates a convoluted framework, however, with no guarantee of further action or enforcement by the Attorney General or FTC. Ultimate imposition of consequences would only occur upon successful action by these public actors. Currently proposed reforms also lack formal mechanisms to require the FTC to collaborate with the DOE when addressing student privacy problems. The FTC and Attorney General do not have expertise in the dynamics of education technology and information flow, the needs of educational institutions and agencies, and the norms of the context.

Direct regulation of data recipients would ensure accountability more clearly, simply, and efficiently. Such regulation would not put schools in an untenable position where they are required to uncover, monitor, and second-guess third party information practices. It could also apply to entities like MOOCs, online tutoring platforms, and educational apps that also use student information but are currently only under a commercial regulatory regime.

CONCLUSION

Reforms can certainly make FERPA's notice and consent provisions more effective and its requirements more comprehensive. Ed-

258. *See id.*

259. *See, e.g.*, S. 1341, 114th Cong. § 5 (2015).

260. S*ee, e.g.*, H.R. 3157 § 11.

261. *Id.*

ucational institutions can improve transparency, including a much more detailed accounting of student data flow, the legitimate educational interest served by disclosure to third parties, the criteria for determining this interest, and de-identification and retention policies. Policymakers could refine the standards for appropriate information management protocols, security, and legitimate educational interests.

However, policymakers should shift their primary focus away from FERPA and its FIPPs-based privacy protection and instead seek to ensure baseline security, governance, and substantive rules through direct regulation that makes data users and recipients accountable for the misuse or mismanagement of student information. These approaches will address privacy concerns and broader contextual considerations more transparently and efficiently, providing stakeholders with a measure of trust in educational institutions and technology providers. This reassurance regarding the privacy and protection of student information is crucial in cultivating the acceptance of data-driven education and all the benefits it may provide.

At the same time, indirectly regulating non-educational actors through FERPA's data recipient requirements is both ineffective and burdensome. Addressing non-educational actors directly, whether through formal statutes or regulation, would be far more efficient and transparent.

Policymakers must also consider both individual and collective interests in imposing procedural and substantive constraints on educational institutions and agencies, as well as outside parties with access to student information. Education has an immense impact on America's democratic governance, equality, economic prosperity, professional opportunity, and individual self-fulfillment. In this case, privacy is not a luxury but a necessity to uphold the public good.