

# The Limits of Education Purpose Limitations

ELANA ZEIDE\*

*While student privacy has been a public issue for half a century, its contours change in response to social norms, technological capabilities, and political ideologies. The Family Educational Rights and Privacy Act (FERPA) seeks to prevent inaccurate or inappropriate information about students from being incorporated into pedagogical, academic, and employment decisionmaking. It does so by controlling who can access education records and, broadly, for what purposes.*

*New education technologies take advantage of cloud computing and big data analytics to collect and share an unprecedented amount of information about students in classrooms. Schools rely on outside, often for-profit, entities to provide these innovative tools. With the shift from education records to student data systems, privacy protection through access control does not account for the possibility that authorized recipients, or even educators themselves, might use student data for commercial or other non-educational purposes.*

---

\* Associate Research Scholar, Princeton University and Visiting Fellow, Yale Law School. I would like to thank my colleagues at the Center for Information Technology, as well as Julia Angwin, Kwaku Akowuah, Alessandro Acquisti, Jack Balkin, danah boyd, Kiel Brennan-Marquez, Monica Bulger, Ryan Calo, Julie Cohen, Kate Crawford, Adam Eisgrau, Michael Froomkin, Jessie Gabriel, Chris Hoofnagle, Sue Glueck, Woodrow Hartzog, Michael Hawes, Sarah Holland, Meg Jones, Margot Kaminski, Brenda Leong, Leonard Niehoff, Helen Nissenbaum, Frank Pasquale, Jules Polonetsky, Joel Reidenberg, Neil Richards, Heather Ross, Evan Selinger, Joe Stephens, Rob Sherman, Daniel Solove, Kathleen Styles, Omer Tene, Amelia Vance, Shane Witnov, and Heather West.

*Both FERPA and new state reforms rely on education purpose limitations as a compromise that allows schools to outsource data-reliant functions while addressing stakeholder concerns. However, current regulations define “education purposes” as information practices conducted on behalf of schools or pursuant to their authorization. Accordingly, they provide more procedural than substantive constraints.*

*As with student privacy protections based on controlling access to education records, modern technological affordances limit the protection provided by education purpose limitations. Data-driven education tools change the nature of student information, the structure and method of school decisionmaking, and the creation of academic credentials. Broad education purpose limitations provide limited protection under these circumstances because they (1) treat education and non-education purposes as binary and mutually exclusive; (2) presume data practices serving education purposes align with students’ academic interests; (3) overlook the ethical complications created by “beta” education; (4) neglect the pedagogical effects of computerized instructional tools; and (5) discount the impact of data-driven technology on education itself. Ethical discourse regarding education technology points to productive avenues for more substantive student privacy protection.*

INTRODUCTION .....	496
I. PROTECTING EDUCATION RECORDS THROUGH ACCESS	
CONTROL .....	498
A. <i>Privacy Concerns Originally Focused On Information Accuracy and Ad Hoc Disclosure</i> .....	498
B. <i>Student Privacy as Access Control</i> .....	499
C. <i>FERPA Delegates Privacy Decisionmaking to Schools</i> .....	501
II. THE SHIFT FROM EDUCATION RECORDS TO	
STUDENT DATA SYSTEMS .....	503
A. <i>Paper Education Records Have Built-in Privacy</i> ....	504
B. <i>Digitally-Mediated Education Technology Captures New Information in Classrooms</i> .....	505

C. <i>Education Data-Mining Collects Information from Unexpected Sources</i> .....	506
D. <i>Networked and Cloud Computing Allows Passive Disclosure</i> .....	508
E. <i>Access Control Does Not Address Contemporary Data Concerns</i> .....	509
III. FROM ACCESS CONTROL TO PURPOSE LIMITATIONS .....	510
A. <i>Amplifying Access Control</i> .....	511
B. <i>Providing Education Purpose Limitations</i> .....	512
IV. THE LIMITS OF EDUCATIONAL PURPOSE LIMITATIONS ...	513
A. <i>Treats Education and Non-Education Purposes as Binary and Mutually Exclusive</i> .....	514
B. <i>Presumes Data Practices Serving Education Purposes Aligns with Students' and Broader Academic Interests</i> .....	514
C. <i>Overlooks the Ethical Complications Created By "Beta" Education</i> .....	516
D. <i>Neglects the Pedagogical Effects of Data-Driven Education</i> .....	517
1. PERVASIVE SURVEILLANCE .....	517
2. EMBEDDED ASSESSMENT .....	518
3. PERMANENT RECORDS .....	520
E. <i>Discounts How Data-Driven Education Technology Shapes Education Itself</i> .....	521
V. PATHS FORWARD: ETHICAL QUESTIONS AND NORMATIVE PRINCIPLES .....	524
CONCLUSION .....	527

## INTRODUCTION

Education technology is changing how, where, when, and what students learn. These new tools may make education more effective, affordable, and connected to the circumstances of specific students. However, this new technology also amplifies concerns about unauthorized access to and commercial use of personally identifiable student information.<sup>1</sup>

---

<sup>1</sup> See 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/> [hereinafter *Joel Reidenberg Interview*]; Jules Polonetsky & Omer

In previous work, I detailed the ways that modern education technology and big data analytics undermine FERPA's student privacy protection.<sup>2</sup> In theory, the statute relies on parental consent to ensure appropriate information practices. In practice, it delegates most of these decisions to schools with minimal transparency and accountability.<sup>3</sup> Schools now routinely share student data with outside technology providers under the statute's broad school official exception.

Here, I continue my inquiry into technologies' impact on the student privacy protections with a focus on education purpose limitations. Both long-standing and recent reforms rely on purpose limitations to facilitate everyday school disclosure to companies providing core education technologies. The efficacy of these restrictions depends on the assumption that serving education purposes also promotes students' interests and the values of the education system.

I contend that reliance on education purpose limitations does not account for the potentially problematic consequences and ethical considerations raised by data use by schools and their approved agents for "educational purposes." Like FERPA's "legitimate education interests" requirement for the school official exception, new reforms equate educational purpose with actions performed by educators or with school direction or approval. This provides more procedural than substantive protection.

To support this claim, Part I examines how FERPA conceptualizes student privacy in terms of access to personally identifiable information. Part II chronicles the change in school information flow created by data-driven technologies. It then describes how the shift from education records to student data systems undermines the efficacy of controlling access as a means to protect student privacy. Part III sets forth the regulatory response to these changes. Most rely on educational purpose limitations to accommodate school reliance on

---

Tene, *Who Is Reading Whom Now: Privacy in Education from Books to MOOCs*, 17 VAND. J. ENT. & TECH. L. 927, 965–69 (2014) [hereinafter Polonetsky & Tene, *Who Is*]; Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 353–55 (2016) [hereinafter Zeide, *Student Privacy*]. See also Jules Polonetsky & Omer Tene, *The Ethics of Student Privacy: Building Trust for Ed Tech*, 21 INT'L REV. INFO. ETHICS 25, 29, 31 (2014) [hereinafter Polonetsky & Tene, *The Ethics*].

<sup>2</sup> See e.g., Zeide, *Student Privacy*, *supra* note 1 at 343, 374.

<sup>3</sup> See e.g., *id.*

outside vendors' education services while addressing concerns about commercial access to and use of information in education records. Part IV enumerates limits of relying on education purpose limitations to promote students' education interests. Part V suggests that student privacy protection incorporates more notably broad purpose limitations: (1) treat education and non-education purposes as binary and mutually exclusive; (2) presume data practices serving education purposes align with students' academic interest; (3) overlook the ethical complications created by "beta" education; (4) neglect the pedagogical effects of computerized instructional tools; and (5) discount the impact of data-driven technology on education itself.

#### I. PROTECTING EDUCATION RECORDS THROUGH ACCESS CONTROL

Student privacy reforms were initially aimed at providing greater transparency and confidentiality.<sup>4</sup> These provisions reflect a default norm that only parents and educators, or recipients serving educational interests on their behalf, have access to student information.<sup>5</sup>

##### A. *Privacy Concerns Originally Focused On Information Accuracy and Ad Hoc Disclosure*

Traditional student privacy protection focuses on limiting access to education records because of their potential impact on judgments regarding students' character, academic performance, and career prospects. In the late 1960s and early 1970s, schools began to collect more and more types of information.<sup>6</sup> They had expanded their offerings and conception of what aspects of students' lives might affect academic performance.<sup>7</sup> This was partly a response to reform that sought to serve the "whole child."<sup>8</sup> In some cases, schools de-

---

<sup>4</sup> See *id.* at 381.

<sup>5</sup> See *id.* at 374–78.

<sup>6</sup> 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].

<sup>7</sup> See *id.*; RUSSELL SAGE REPORT, *supra* note 6, at 13–15.

<sup>8</sup> See Zeide, *Student Privacy*, *supra* note 2, at 355.

nied parents and students access to students' records for fear of creating self-fulfilling prophecies.<sup>9</sup> The media reported instances where educators' idiosyncratic interpretation of student behavior had severe academic consequences that might impact future opportunities and employment.<sup>10</sup> Parents feared that secret files would create an erroneous permanent record that could have "devastatingly negative effects on the academic future and job prospects of an innocent, unaware student."<sup>11</sup> Most schools had no procedures or protocols governing disclosure of potentially sensitive information to parents, students, other educators, and outsiders.<sup>12</sup> New York Senator James Buckley proposed the first and primary federal student privacy law, FERPA, to remedy an environment where there were "frequent, even systematic violations of the privacy of students and parents by the schools through . . . the unauthorized, inappropriate release of personal data to various individuals and organizations."<sup>13</sup>

### B. Student Privacy as Access Control

This background shaped FERPA's regulatory mechanisms. The statute seeks to prevent these harms by controlling access to student information. It specifically covers personally identifiable student information in education records<sup>14</sup> maintained by schools

---

<sup>9</sup> See Divoky, *supra* note 6, at 18–21.

<sup>10</sup> See *id.*

<sup>11</sup> 120 CONG. REC. 14,580 (1974) (statement of Sen. Buckley). See also *id.* at 39,863 (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.").

<sup>12</sup> See *id.* at 14,581 (statement of Sen. Buckley) (articulating his proposed amendments that sought "to restore parental rights and to protect privacy."); see also Senator James L. Buckley, Speech Before the Legislative Conference of the National Congress of Parents and Teachers (Mar. 12, 1975) reprinted in 121 CONG. REC. 13,990 (1975) [hereinafter Buckley Speech] ("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.").

<sup>13</sup> Buckley Speech, *supra* note 12, at 13,991.

<sup>14</sup> See 20 U.S.C. § 1232g(a)–(b) (2012). 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" created in its

and districts<sup>15</sup> that receive federal funding.<sup>16</sup> FERPA tries to ensure the accuracy of student information by giving parents and eligible students<sup>17</sup> the right to access education records and challenge their accuracy.<sup>18</sup> It also gives parents the right to consent to educational agency or institution disclosure of personally identifiable student information<sup>19</sup> subject to several exceptions.<sup>20</sup> Some exceptions permit education actors to respond to legal requests and act quickly in cases of emergency.<sup>21</sup> The other exceptions can be broadly characterized

---

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 which relate exclusively to [the individual] in that [individual’s] capacity as an employee and are not available for use for any other purpose.” *Id.* at § 1232g(a)(4)(B)(i)–(iii).

<sup>15</sup> *See id.* at § 1232g(a)(3), (4)(A). 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.* at § 1232g(a)(3).

<sup>16</sup> The bill was introduced as an extension to the Secondary Education Act, which controls federal funding for schools. *See* Buckley Speech, *supra* note 12, at 13,990. FERPA technically does not require education institutions and agencies to adhere to its provisions. *See generally* 20 U.S.C. § 1232g. Instead it conditions federal funding on compliance (defined as education institutions and agencies not demonstrating a policy or practice of FERPA violations). *See generally id.* Few, if any, schools would be economically feasible without federal support, so references to FERPA are generally phrased as if the statute affirmative prohibits non-compliant action. *See id.* at § 1232g(a)(1)(A)–(B).

<sup>17</sup> *See* 20 U.S.C. at § 1232g(d). Students can exercise their own rights under FERPA when they reach the age of 18 or enter post-secondary education. *Id.* For the purposes of brevity, references regarding parents’ rights and concerns in this paper also include those of eligible students.

<sup>18</sup> *See id.* at § 1232g(a)(1)–(2).

<sup>19</sup> *See id.* at § 1232g(b)(2). *See also* 34 C.F.R. § 99.3 (“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 . . .”).

<sup>20</sup> *See generally* 34 C.F.R. § 99.31 (describing under what circumstances prior consent is not required to disclose student information). As of July 2016, FERPA has eighteen exceptions to the consent for disclosure requirement. *See generally* 34 C.F.R. at pt. 99. These exceptions, which have been added to the statute over time, permit schools to disclose information without consent in response to legal proceedings and law enforcement requests and ensure student safety. *Id.*

<sup>21</sup> *See* Letter from Arne Duncan, Sec’y of Educ., U.S. Dep’t of Educ., to Edward J. Markey, Senator, U.S. Senate, at 3 (Jan. 13, 2014). Secretary of Education

as proxies for whether access to covered information serves educational interests.<sup>22</sup> FERPA permits disclosure without consent to recipients including (1) other schools where students apply or transfer to; (2) entities entrenched in the education system like accrediting organizations; and (3) third parties acting on a school's behalf and serving legitimate educational interests or defined educational purposes.<sup>23</sup>

### C. FERPA Delegates Privacy Decisionmaking to Schools

FERPA delegates a substantial amount of discretion to educators and administrators in determining the appropriate circumstances for disclosure. The statute's trust in educational entities is most obvious in the school official exception that governs most day-to-day disclosure of personally identifiable student information to outside vendors that provide email, cafeteria management, and data management systems.<sup>24</sup>

The exception allows schools and districts to disclose covered information without parental consent to "school officials, including teachers, within the agency or institution" who have what the school has determined to be "legitimate educational interests" in the information. Schools must also maintain "direct control" over student information, which can be accomplished contractually.<sup>25</sup> They do not need to record instances of disclosure to do so,<sup>26</sup> but recipients generally cannot re-disclose covered information except as directed by schools.<sup>27</sup>

FERPA also exhibits significant faith in school discretion through its "directory information" exception. The statute allows educators—classroom teachers and school administrators—to share

---

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." *Id.*

<sup>22</sup> See Zeide, *Student Privacy*, *supra* note 1, at 358.

<sup>23</sup> 34 C.F.R. § 99.31.

<sup>24</sup> See Zeide, *Student Privacy*, *supra* note 1, at 354.

<sup>25</sup> *Id.* at § 99.31(a)(1)(i)(A).

<sup>26</sup> See *id.* at § 99.32(d).

<sup>27</sup> See *id.* at § 99.33(a)(1).



student information that the school designates as directory information, subject to student or parental opt-out.<sup>28</sup> Directory information can include fairly innocuous information like names, addresses, and birthdates, but also more sensitive information such as an athlete's weight and school activities or clubs.<sup>29</sup>

FERPA requires that schools inform students and parents about disclosure under these exceptions in an annual notice, including what categories of data are considered "directory information," who qualifies as a "school official," and what constitutes a "legitimate educational interest."<sup>30</sup> Following ED's model language, schools have broad discretion in defining these terms.<sup>31</sup> As noted by the National Center for Education Statistics, the statute "does not say

---

<sup>28</sup> See generally *id.* at § 99.37(a).

<sup>29</sup> The model language states that "[t]he primary purpose of directory information is to allow the **[School or School District]** to include information from your child's education records in certain school publications. Examples include:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks." *Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information*, U.S. DEP'T EDUC., <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html> (last modified Dec. 19, 2014) [hereinafter *Model Notice for Directory Information*] (bold text in original).

<sup>30</sup> 34 C.F.R. §§ 99.37, 99.7.

<sup>31</sup> See Zeide, *Student Privacy*, *supra* note 1, at 343. See also *Model Notification of Rights Under FERPA for Elementary and Secondary Schools*, U.S. DEP'T EDUC., <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html> (last modified Dec. 22, 2014) [hereinafter *FERPA for Elementary and Secondary Schools*]; *Model Notification of Rights Under FERPA for Postsecondary Institutions*, U.S. DEP'T EDUC., <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html> (last modified Jan. 2, 2015) [hereinafter *FERPA for Postsecondary Institutions*].

specifically who those persons are, nor does it stipulate how to determine the limits of a legitimate educational interest.”<sup>32</sup>

FERPA’s compliance-oriented enforcement emphasizes the amount of trust placed in educational institutions.<sup>33</sup> FERPA does not impose any direct accountability on schools for individual FERPA violations.<sup>34</sup> It instead requires that schools or districts exhibit a “policy or practice” of denying parents or eligible students their rights under the statute as the threshold for enforcement.<sup>35</sup> ED has never exercised its option to withdraw federal funding in the course of the statute’s forty-year history.<sup>36</sup>

## II. THE SHIFT FROM EDUCATION RECORDS TO STUDENT DATA SYSTEMS

Over time, new technologies have changed the type of information collected, how it flows through schools, and who considers it valuable.<sup>37</sup> The move from education records to student data reduces the efficacy of regulatory mechanisms that rely on controlling access.<sup>38</sup> In theory, FERPA should result in information

---

<sup>32</sup> *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies*, NAT’L CTR. FOR EDUC. STAT. 1 (March 2004), <http://nces.ed.gov/pubs2004/2004330.pdf>.

<sup>33</sup> See Zeide, *Student Privacy*, *supra* note 1, at 360. See also Stephanie Humphries, *Institutes of Higher Education, Safety Swords, and Privacy Shields: Reconciling FERPA and the Common Law*, 35 J.C. & U.L. 145, 158 (2008).

<sup>34</sup> See *Gonzaga Univ. v. Doe*, 536 U.S. 273, 290 (2002) (“FERPA’s nondisclosure provisions contain no rights-creating language . . . [and] therefore create no rights enforceable . . .”).

<sup>35</sup> See 20 U.S.C. § 1232g(b)(1)–(2). 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. See 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.”).

<sup>36</sup> See *Joel Reidenberg Interview*, *supra* note 1.

<sup>37</sup> See 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>.

<sup>38</sup> See Elana Zeide, *19 Times Data Analysis Empowered Students and Schools: Which Students Succeed and Why?*, FUTURE OF PRIVACY F. 7, 13–14 (Mar. 22, 2016), [https://fpf.org/wp-content/uploads/2016/03/Final\\_19Times-Data\\_Mar2016-1.pdf](https://fpf.org/wp-content/uploads/2016/03/Final_19Times-Data_Mar2016-1.pdf) [hereinafter Zeide, *19 Times*].

flow that does not permit outsiders access to personally identifiable student information unless they are performing services for schools that have determined such disclosure serves a legitimate educational interest. In practice, the statute no longer provides meaningful transparency to enable student and parental oversight of information accuracy or informed consent.<sup>39</sup>

#### A. *Paper Education Records Have Built-in Privacy*

Until recently, technology could not capture detailed information about students' behavior and performance in the classroom. In traditional physical school environments, teachers "collect" information about students when they answer questions in class, complete assignments, or take tests. Teachers also receive and interpret sensory data generated as students interact in the classroom: their expressions, vocal tone, clothing, health, posture, and interaction with classmates. This input helps teachers assess and diagnose student progress, known as formative assessment.<sup>40</sup>

Only a small portion of the information exchanged in classrooms could be memorialized on paper records—typically written assignments, tests, or teachers' personal notes. Schools would incorporate end-of-term grades into official records and create credentials, like transcripts, that indicated course enrollment, professors, credits earned, and grades. They stored this information in files located on school property, along with basic administrative information.<sup>41</sup> Disclosure occurred by physically permitting access to, transferring, or verbally communicating student information to occasional outside recipients.<sup>42</sup>

---

<sup>39</sup> Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 343, 374 (2016) [hereinafter Zeide, *Student Privacy*].

<sup>40</sup> *See id.*

<sup>41</sup> *See, e.g.*, U.S. DEP'T EDUC., FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) FINAL RULE 34 CFR PART 99: SECTION-BY-SECTION ANALYSIS 6 (Dec. 2008), available at <http://www2.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf> ("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 . . .").

<sup>42</sup> *See* Zeide, *Student Privacy*, *supra* note 1, at 375.

### B. Digitally-Mediated Education Technology Captures New Information in Classrooms

The interactivity of online platforms and mobile devices has spurred tremendous change in education environments. New educational technologies collect, process, and create much more information about students in much greater detail.<sup>43</sup> Today's education technology allows schools to capture information about students' moment-to-moment interaction with learning platforms, creating digital artifacts instead of sensory impressions.<sup>44</sup> This includes not only the content of their performance, but metadata that can show how many times a student has logged into a system and how long it took the student to answer a given question.<sup>45</sup>

Because of these innovations, student records include new variables about students and their behavior. Educators have come to realize that non-cognitive or "soft" skills like resilience and teamwork have an important impact on student achievement.<sup>46</sup> As a result, some educators now collect psychometric data as a means to capture a broader array of student characteristics that may affect student achievement.<sup>47</sup> Schools now collect significantly more information

---

<sup>43</sup> See Natasha Singer, *Big Data Means Big Questions on How That Information is Used*, N.Y. TIMES: BITS (Mar. 3, 2014, 3:12 PM), <http://bits.blogs.nytimes.com/2014/03/03/big-data-means-big-questions-on-how-that-information-is-used/>.

<sup>44</sup> See generally Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, FORDHAM L. SCH. CTR. L. & INFO. POL'Y 1 (2013).

<sup>45</sup> FAZEL KESHTKAR ET AL., *Analyzing Students' Interaction Based on Their Responses to Determine Learning Outcomes* in PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON EDUCATIONAL DATA MINING 588–89 (2015).

<sup>46</sup> OFFICE OF EDUC. TECH., U.S. DEP'T OF EDUC., *Promoting Grit, Tenacity and Perseverance: Critical Factors for Success in the 21st Century* (Feb. 14, 2013) (draft); Julie Scelfo, *Angela Duckworth on Passion, Grit and Success*, THE N.Y. TIMES (Apr. 8, 2016), <https://www.nytimes.com/2016/04/10/education/edlife/passion-grit-success.html>.

<sup>47</sup> See, e.g., 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>; EMMETT MCGROARTY, JOY PULLMANN, & JANE ROBBINS, PIONEER INST. CTR. FOR SCH. REFORM, COGS IN THE MACHINE: BIG DATA, COMMON CORE AND NATIONAL TESTING 11 (May 2014), [http://www.stopcossinnys.com/uploads/Cogs\\_in\\_the\\_Machine.pdf](http://www.stopcossinnys.com/uploads/Cogs_in_the_Machine.pdf); ALEX MOLNAR ET AL., NAT'L EDUC. POL'Y CTR., SCHOOLHOUSE COMMERCIALISM LEAVES POLICYMAKERS BEHIND—THE SIXTEENTH ANNUAL

about students and incorporate new types of information into education records.<sup>48</sup>

*C. Education Data-Mining Collects Information from  
Unexpected Sources*

Schools increasingly incorporate new data sources. In addition to classroom observation, students are subject to geographic, financial, health, and social media monitoring.<sup>49</sup> Schools can scour social media to deal with cyberbullying, detect cheating, and identify suicidal, violent, or disengaged students for intervention.<sup>50</sup> In addition, schools use traditional surveillance technologies such as cameras in hallways for safety<sup>51</sup> or in classrooms to avoid student

---

REPORT ON SCHOOLHOUSE COMMERCIALIZING TRENDS: 2012–2013 28 (Mar. 2014), <http://nepc.colorado.edu/files/trends-2013.pdf>; Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 17, 2014, 1:32 PM), <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, 3:45 PM), <http://www.politico.com/story/2014/05/student-data-privacy-market-106692.html>. See also Press Release, Common Sense Media, National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared (Jan. 22, 2014), available at <https://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern>; Quinten Plummer, *Apps Still Tracking Kids Despite Privacy Laws*, TECH TIMES (Dec. 8, 2014, 11:38 PM), <http://www.techtimes.com/articles/21766/20141208/apps-still-tracking-kids-despite-privacy-laws.htm>; see Natasha Singer, *Deciding Who Sees Students' Data*, THE N.Y. TIMES, (Oct. 5, 2013), [http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?\\_r=0](http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?_r=0) [hereinafter Singer, *Deciding*]

<sup>48</sup> See Polonetsky & Tene, *Who Is*, *supra* note 1, at 941. See also Polonetsky & Tene, *The Ethics*, *supra* note 1, at 28–29.

<sup>49</sup> See Barnes, *supra* note 37.

<sup>50</sup> William Tucker and Amelia Vance, *School Surveillance: The Consequences for Equity & Privacy*, EDUC. LEADERS REP. 6-7, available at [http://www.nasbe.org/wp-content/uploads/Tucker\\_Vance-Surveillance-Final.pdf](http://www.nasbe.org/wp-content/uploads/Tucker_Vance-Surveillance-Final.pdf).

<sup>51</sup> See, e.g., Brian R. Warnick, *Surveillance Cameras in Schools: An Ethical Analysis*, 77 HARV. EDUC. REV. 317, 319 (2007); Kevin P. Brady, “Big Brother” Is Watching, But Can He Hear, Too?: Legal Issues Surrounding Video Camera Surveillance and Electronic Eavesdropping in Public Schools, 218 WEST EDUC. L. REP. 1, 5 (2007).

abuse.<sup>52</sup>

The “Internet of Things” incorporates even more information into the student records.<sup>53</sup> Online proctoring platforms may include video, facial recognition, audio, and biometric information as a means to verify student identity and monitor assessments at scale.<sup>54</sup> Some schools, particularly residential college campuses, provide students with Radio Frequency Identification-enabled cards to access to campus facilities and pay for items in school-managed cafeterias and stores.<sup>55</sup> Schools track students’ health and movements and calorie expenditure with Fitbits.<sup>56</sup> Reformers have visions of machines that will track students’ eyes to determine when they are “engaged” and track pulses in order to examine student stress levels

---

<sup>52</sup> See, e.g., Mackenzie Ryan, *Body Cameras Making Their Way into Iowa Schools*, DES MOINES REG. (July 5, 2015, 9:47 PM), <http://www.desmoinesregister.com/story/news/education/2015/07/05/body-cameras-burlington-schools/29746803/>.

<sup>53</sup> See Itai Asseo et al., *The Internet of Things: Riding the Wave in Higher Education*, EDUCAUSE REV. 12 (2016) available at <http://er.educause.edu/~media/files/articles/2016/6/erm1641.pdf>.

<sup>54</sup> See, e.g., Natasha Singer, *Online Test-Takers Feel Anti-Cheating Software’s Uneasy Glare*, N.Y. TIMES (Apr. 5, 2015), <http://www.nytimes.com/2015/04/06/technology/online-test-takers-feel-anti-cheating-software-uneasy-glare.html> [hereinafter Singer, *Online*].

<sup>55</sup> See, e.g., Mary Catherine O’Connor, *Northern Arizona University to Use Existing RFID Student Cards for Attendance Tracking*, RFID J. (May 24, 2010), <http://www.rfidjournal.com/articles/pdf?7628>. But see David Kravets, *Tracking School Children with RFID Tags? It’s All About the Benjamins*, WIRED, (Sept. 7, 2012, 6:30 AM), <https://www.wired.com/2012/09/rfid-chip-student-monitoring/> (reflecting the uncommonness of using RFID tags in the school setting).

<sup>56</sup> See, e.g., Jessica Chasmar, *Oklahoma University Requires Freshmen to Wear Fitbit, Track 10K Steps Per Day*, THE WASH. TIMES (Jan. 11, 2016), <http://www.washingtontimes.com/news/2016/jan/11/oklahoma-university-requires-freshmen-to-wear-fitbit/>.

over the course of instruction.<sup>57</sup> The potential breadth and detail of this collection of information about students is unprecedented.<sup>58</sup>

The founder of Knewton, one of the most prominent personalized analytics providers, boasted in 2012:

We literally know everything about what you know and how you learn best, everything. Because we have five orders more magnitude of data about you than Google has. We literally have more data about our students than any company has about anything, and it's not even close.<sup>59</sup>

#### D. Networked and Cloud Computing Allows Passive Disclosure

Schools increasingly rely on networked and cloud computing platforms as an essential part of their everyday instruction and administration. Information is stored digitally, allowing for seamless data sharing.<sup>60</sup>

At a classroom level, teachers frequently integrate applications into their instruction, classroom management, and curricular development.<sup>61</sup> These include everything from math instructional modules to behavioral tracking systems to student-specific social media platforms.<sup>62</sup> This growth in the use of third parties to supplement

---

<sup>57</sup> CHRISTOPHER WAS ET AL., EYE-TRACKING TECHNOLOGY APPLICATIONS IN EDUCATIONAL RESEARCH (2016); Stephanie Simon, *Biosensors to Monitor U.S. Students' Attentiveness*, REUTERS (Jun. 13, 2012), <http://www.reuters.com/article/us-usa-education-gates-idUSBRE85C17Z20120613>; *Eye Tracking in Education and Educational Research*, TOBII PRO (Jun. 21, 2015), <http://www.tobiiipro.com/fields-of-use/education/>.

<sup>58</sup> See Leo Hohmann, *More Evidence of Invasive Student Data-Mining Scheme*, WND (Dec. 4, 2014, 7:44 PM), <http://www.wnd.com/2014/12/more-evidence-of-invasive-student-data-mining-scheme/>.

<sup>59</sup> Jose Ferreira, *Knewton – Education Datapalooza*, YOUTUBE (Nov. 3, 2012), [https://www.youtube.com/watch?v=Lr7Z7ysDluQ&feature=youtube\\_gdata\\_player](https://www.youtube.com/watch?v=Lr7Z7ysDluQ&feature=youtube_gdata_player).

<sup>60</sup> See *Data in the Cloud: A Legal and Policy Guide for School Boards on Student Privacy in the Cloud Computing Era*, NAT'L SCH. BOARDS ASS'N 1, 2 (Apr. 2014), <http://edu.safegov.org/media/2014-04-NSBA-Data-in-the-Cloud-Legal-and-Policy-Guide.pdf> [hereinafter *Data in the Cloud*].

<sup>61</sup> See *Teacher Apps Raise Student Privacy Concerns*, CONNECT LEARNING TODAY (Mar. 25, 2015), <http://connectlearningtoday.com/teacher-apps-raise-student-privacy-concerns> [hereinafter *Teacher Apps Raise*].

<sup>62</sup> *Id.*

educational practice is not limited to the classroom: administrators outsource data-reliant operational functions like cafeteria services and e-billing technology to take advantage of the expertise of specialized service providers and companies.<sup>63</sup> The majority of outside entities providing digital-reliant services are for-profit entities rather than the traditional public and non-profit actors in the American education system.<sup>64</sup>

As more and different types of data are collected, that data is often kept without review, leading to an information ecosystem where education records may be full of extraordinarily detailed data about students on cloud computing networks that no human has ever seen.<sup>65</sup> As Princeton computer science professor Edward Felten noted, “If storage is free but analysts’ time is costly, then the cost-minimizing strategy is to record everything and sort it out later.”<sup>66</sup>

#### *E. Access Control Does Not Address Contemporary Data Concerns*

FERPA’s mechanisms reflect the era in which it was passed. They rely the built in limitations of physically-bound data.<sup>67</sup> It is silent on many realities of today’s information technology, like metadata.<sup>68</sup> The statutes, rules, and definitions do not map well on modern technology, so educators and even experts remain uncertain

---

<sup>63</sup> For example, educators might use sensors to track students’ eye movement while reading to detect possible learning disabilities, facilitate access to school buildings with identification cards, or identify students with face or palm scans. See Polotensky & Tene, *Who Is*, *supra* note 1, at 935 n.10.

<sup>64</sup> See, e.g., Diane Ravitch, *Is inBloom Engaged in Identify Theft?*, DIANE RAVITCH’S BLOG (Apr. 7, 2013), <https://dianeravitch.net/2013/04/07/is-inbloom-engaged-in-identity-theft/> [hereinafter Ravitch, *Identity Theft*]; Diane Ravitch, *Promise and Peril: Technology Can Inspire Creativity or Dehumanize Learning*, SCI. AM., Aug. 1, 2013, at 66; MOLNAR ET AL., *supra* note 47, at 29.

<sup>65</sup> See *Data in the Cloud*, *supra* note 60, at 1.

<sup>66</sup> David Von Drehle, *The Surveillance Society*, TIME.COM (August 1, 2013), <http://nation.time.com/2013/08/01/the-surveillance-society>.

<sup>67</sup> See Zeide, *Student Privacy*, *supra* note 1, at 343–44; *supra* Section II.A.

<sup>68</sup> See 34 C.F.R. § 99.31(b) (reflecting that metadata is not protected under 34 C.F.R. pt. 99 to the extent that the data is de-identified); PRIVACY TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 2–3 (Feb. 25, 2014), <https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf>.



as to the contours of its protection.<sup>69</sup> The networks that allow automatic transfer and storage of vast quantities of very detailed information make it difficult for schools to keep track of and notify parents or eligible students regarding what information is disclosed, to whom it is disclosed, and what data practices the recipients employ.<sup>70</sup>

Educators and administrators, especially at the classroom level, may share information with companies without understanding what the information is they are sharing, with whom, and the terms of use that apply. Many of these platforms and applications are free, or only require payment for certain upgrades, which means they can be adopted by teachers independently without school or district approval.<sup>71</sup> Some districts have started to implement app vetting systems to ensure that these tools have appropriate privacy and security practices, but even the most sophisticated and well-funded of these efforts struggle to keep up with the quantity of outside applications, the variety of their policies, and ever-emerging technological affordances.<sup>72</sup>

### III. FROM ACCESS CONTROL TO PURPOSE LIMITATIONS

Amplified privacy concerns prompted a flood of state legislation and executive action.<sup>73</sup> Since 2013, 527 student privacy bills have

---

<sup>69</sup> See LYNDSEY PINKUS & ALEXANDRIA BARKMEIER, *COMPLYING WITH FERPA AND OTHER FEDERAL PRIVACY AND SECURITY LAWS AND MAXIMIZING APPROPRIATE DATA USE: A STATE POLICYMAKER'S GUIDE 3* (2013), <http://dataqualitycampaign.org/wp-content/uploads/2016/03/Complying-with-FERPA-03.2013.pdf>.

<sup>70</sup> See *Teacher Apps Raise*, *supra* note 61.

<sup>71</sup> See Natasha Singer, *Privacy Pitfalls as Education Apps Spread Haphazardly*, THE 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> [hereinafter Singer, *Privacy Pitfalls*].

<sup>72</sup> See *id.*

<sup>73</sup> See Benjamin Herold, *FERPA Update Sought as Part of Federal Student-Data-Privacy Protection Efforts*, EDUC. WK. (Feb. 12, 2015, 3:14 PM), [http://blogs.edweek.org/edweek/DigitalEducation/2015/02/ferpa\\_update\\_student\\_data\\_privacy.html?cmp=SOC-SHR-FB](http://blogs.edweek.org/edweek/DigitalEducation/2015/02/ferpa_update_student_data_privacy.html?cmp=SOC-SHR-FB). See also Ariel Bogle, *Obama Proposes New Protections for Student Data*, SLATE: FUTURE TENSE (Jan. 12, 2015, 4:44 PM), [http://www.slate.com/blogs/future\\_tense/2015/01/12/obama\\_announces\\_student\\_digital\\_privacy\\_act\\_at\\_ftc.html](http://www.slate.com/blogs/future_tense/2015/01/12/obama_announces_student_digital_privacy_act_at_ftc.html); Benjamin Herold, *Arne Duncan Responds to Criticism Over Student Data Privacy*, EDUC. WK. (Apr. 15, 2014, 9:59

been introduced across forty-nine states, and thirty-eight states have passed ninety-one of those bills into law.<sup>74</sup> In 2015, federal legislators introduced several bills related to student data governance, including several proposed FERPA amendments.<sup>75</sup> ED's Privacy Technical Assistance Center (PTAC) has issued guidance on a range of issues, including best practices for schools to protect student privacy when sharing information with online service providers and for de-identifying student data.<sup>76</sup> Trade, academic, and advocacy organizations have also created independent principles and suggested practices.<sup>77</sup>

#### A. Amplifying Access Control

These reforms represent a wide variety of viewpoints on what harms are at stake, what information practices should be appropriate, and how to best achieve them.<sup>78</sup> Most focus on amplified concerns about problematic practices and potential harm that can occur when vendors collect, capture, analyze, or use student data in the course of providing education-related school services.<sup>79</sup>

Many reforms require schools to be more cognizant and careful about how they share and store student information.<sup>80</sup> Some reforms add stricter requirements to promote better governance and greater protection.<sup>81</sup> As part of proper governance, most reforms require better security protection through more advanced technology and

---

AM), [http://blogs.edweek.org/edweek/DigitalEducation/2014/04/duncan\\_on\\_data\\_privacy\\_technol.html?\\_ga=1.249152903.1821166166.1471729398](http://blogs.edweek.org/edweek/DigitalEducation/2014/04/duncan_on_data_privacy_technol.html?_ga=1.249152903.1821166166.1471729398).

<sup>74</sup> Data on file with author.

<sup>75</sup> Polonetsky & Tene, *Who Is*, *supra* note 1, at 972–73.

<sup>76</sup> *See generally*, PRIVACY TECH. ASSISTANCE CTR., *supra* note 68.

<sup>77</sup> *See, e.g.*, Brenda Leong, *K–12 Student Privacy Pledge Announced*, FUTURE OF PRIVACY F. (Oct. 7, 2014), <http://www.futureofprivacy.org/2014/10/07/k-12-student-privacy-pledge-announced/>.

<sup>78</sup> *See generally Comparison of 2015–2016 Federal Education Data Privacy Laws and Bills*, NAT'L ASS'N OF STATE BD. OF EDUC. 3, <http://www.nasbe.org/wp-content/uploads/2015-2016-Congress-Education-Data-Privacy-Laws-and-Bills-2016.03.31-Public.pdf> (last updated Mar. 31, 2016) [hereinafter NASBE].

<sup>79</sup> *See id.* at 4.

<sup>80</sup> *See, e.g., id.* at 3.

<sup>81</sup> *See, e.g., id.* at 2–3, 8.

educator training.<sup>82</sup> Several expand the scope of the type of data protected.<sup>83</sup> Others seek to abate privacy problems by prohibiting collection of certain types of information and requiring data minimization.<sup>84</sup>

These reforms predominantly restate or amplify FERPA's protections.<sup>85</sup> They expand on current transparency, notice, and consent concerns and aim to further restrict disclosure by expanding the types of information covered, requiring contractual agreements before disclosure, and imposing additional qualification requirements on recipients.<sup>86</sup> They are procedural and governance protections, some of which add direct accountability for non-compliance.<sup>87</sup>

### B. *Providing Education Purpose Limitations*

Like FERPA, many new reforms try to address stakeholders' concerns while accommodating educators' need to share information with outside parties as part of commonplace institutional practice. To do so they rely on purpose limitations similar to the "legitimate educational interests" required by FERPA's school official exception.<sup>88</sup> California's Student Online Personal Information Protection Act ("SOPIPA"), and the related Student Use Privacy in Education Rights Act "SUPER Act," regulates data operators directly and prohibits profiling students for other than "K-12 purposes."<sup>89</sup> This is defined as "purposes that customarily take place at the direction of the K-12 school, teacher, or district." This approach

---

<sup>82</sup> See *id.* at 5.

<sup>83</sup> See *id.* at 2.

<sup>84</sup> See *id.* at 7.

<sup>85</sup> See Zeide, *Student Privacy*, *supra* note 1, at 340.

<sup>86</sup> See *id.* at 344.

<sup>87</sup> See NASBE, *supra* note 78, at 13.

<sup>88</sup> See Polonetsky & Tene, *Who Is*, *supra* note 1, at 932-33, 953-54. See generally Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584(a)-(e) (West 2015); Jules Polonetsky & Joseph Jerome, *Student Data: Trust, Transparency and the Role of Consent*, FUTURE OF PRIVACY F. 6, 15 (Oct. 2014), [https://fpf.org/wp-content/uploads/FPF\\_Education\\_Consent\\_StudentData\\_Oct2014.pdf](https://fpf.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf) [hereinafter Polonetsky & Jerome, *Student Data*]; Leong, *supra* note 77.

<sup>89</sup> SOPIPA prohibits operators from using, selling, disclosing, and engaging in targeted marketing with K-12 student data. See CAL. BUS. & PROF. CODE § 22584(a)-(b).

is, by far, the most common, and has been passed in fifteen states.<sup>90</sup> Colorado takes a more specific approach: data recipients can only use covered information for purposes authorized in contracts with disclosing educational institutions.<sup>91</sup> Georgia's 2015 law takes a slightly more enumerated approach: it defines "K-12 school purposes" as "purposes that take place at the direction of the K-12 school, teacher, or local board of education or aid in the administration of school activities," again leaving wide discretion to the judgment of a school as to the definition of an educational purpose.<sup>92</sup>

These laws do not focus on regulating collection, use, or processing among educators or their approved recipients used for educational purposes.<sup>93</sup> The Student Privacy Pledge, a voluntary pledge for industry, has a similar set-up. It defines "educational purposes" as "services or functions that customarily take place at the direction of the educational institution or agency or their teacher or employee, for which the institutions or agency would otherwise use its own employees, and that aid in the administration or improvement of educational and school activities."<sup>94</sup> While more detailed, this definition again gives almost unlimited discretion to schools and institutions as to what they would customarily do for educational purposes.

#### IV. THE LIMITS OF EDUCATIONAL PURPOSE LIMITATIONS

Educational purpose limitations rest on assumptions that no longer apply in an era of big data. They treat educational and non-educational purposes as mutually exclusive and ignore the ramifications of educators using student data to serve educational purposes in educational settings. Even well-meaning actors who have a legitimate educational interest in accessing student information might nevertheless use data in ways that don't serve students' interests or the broader goals of American education.<sup>95</sup>

---

<sup>90</sup> Data on file with author.

<sup>91</sup> H.R. 1423, 70th Gen. Assemb., 2d Reg. Sess. (Colo. 2016).

<sup>92</sup> GA. CODE ANN., tit. 20 § 20-2-662 (2016).

<sup>93</sup> See Zeide, *Student Privacy*, *supra* note 1, at 379.

<sup>94</sup> *About the Pledge*, STUDENT PRIVACY PLEDGE, <https://studentprivacypledge.org> (last visited March 9, 2017).

<sup>95</sup> See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (defining "privacy" as context-specific appropriate flow of information).

Below I highlight several limits of relying on education purpose limitations. These provide a framework for more normative and substantive approaches to student privacy, as well as productive avenues for further inquiry.

*A. Treats Education and Non-Education Purposes as Binary and Mutually Exclusive*

Education-based purpose restrictions assume that the distinction between educational and non-educational uses are clear. They conceive of a world of binaries and boundaries: information is either “inside” or “outside” institutions and uses and purposes are either “educational” or not. This is no longer the case as entities outside of traditional educational institutions increasingly perform educational functions and educators collect and use data that has as much potential to impact students’ future as formal education records and transcripts did in an era of paper records. The data that schools collect and use can have commercial value to the schools themselves irrespective of third parties, and private entities often have incentives to use data to improve educational outcomes. Student privacy laws and policies based on the assumption of binaries also do not address circumstances when information can be used for both educational and non-educational purposes—for example, when a company uses information from students to provide both immediate instruction and gauge market demand for a new product. As education services moves beyond the classroom walls, so too do the bands of what may be considered an educational purpose. Redrawing these boundaries may be a herculean task.

*B. Presumes Data Practices Serving Education Purposes Aligns with Students’ and Broader Academic Interests*

Purpose limitations presume a unity of interests of those using student information for educational purposes. Until recently, most “educational” uses of student data by educators or approved recipients tended to promote students’ educational interests as well, whether directly or indirectly.<sup>96</sup> Students, for example, benefit when schools share information with accreditors to maintain their accredited status.

---

<sup>96</sup> See Zeide, *Student Privacy*, supra note 1, at 340, 370–71.

Education purpose limitations equate educational functions with acceptable use.<sup>97</sup> This presumption made sense given the limitations of paper education records. The information they contained was primarily useful as administrative tools and credentials.<sup>98</sup> There were very few other ways to employ education records aside from student evaluation.<sup>99</sup> The utility of student data lay in the ability to associate certain information with specific individuals.<sup>100</sup> Historically, data embedded in physical records could not be extracted for easy analysis or aggregation with other information to generate non-educational insights.<sup>101</sup> 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.”<sup>102</sup> As a result, the statute allows schools to share information based on recipients’ established roles within America’s education system.<sup>103</sup>

There is a default expectation in traditional education environments that educators or institutions will use student information in the service of educational aims, whether to advance individual, institutional, or pedagogical interests.<sup>104</sup> Even private universities with very large endowments and profit-generating machines—like intellectual property or sports franchises—still fall under the rubric of organizations whose primary obligation is to their educational mission.

Today, institutional interests may conflict with those of their students. For example, schools can use predictive analytics to identify students to advance several different types of interest. They might, as reformers suggest, use early warnings to prompt institutional intervention aimed at improving students’ grades. However, schools also have an incentive to use predictions to allocate resources away from struggling students to those more likely to stay in school.<sup>105</sup> In

---

<sup>97</sup> *See id.* at 358.

<sup>98</sup> *See id.* at 377.

<sup>99</sup> *See id.*

<sup>100</sup> *See id.* at 355.

<sup>101</sup> *See id.* at 378.

<sup>102</sup> Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public School Children*, 84 NEB. L. REV. 1158, 1203 (2006).

<sup>103</sup> *See supra* Section I.B.

<sup>104</sup> *See id.* at 370–71.

<sup>105</sup> *See* Carl Straumsheim, *Mixed Signals*, INSIDE HIGHER ED. (Nov. 6, 2013, 3:00 AM), <https://www.insidehighered.com/news/2013/11/06/researchers-cast->

a recent example, a university president wanted to pressure the most at-risk freshmen to leave within the first month of school in order to have better student retention for school ranking purposes.<sup>106</sup> These school uses of data (arguably) promote “educational” purposes, but have very different effects on individual students’ academic trajectories.

*C. Overlooks the Ethical Complications Created By  
“Beta” Education*

The experimental and developing nature of data-driven education technology used for educational purposes raises ethical questions. There are few research studies showing that new technologies will provide better outcomes for students, schools, or the education system overall.<sup>107</sup> Many new data-driven education technologies have not been thoroughly vetted.<sup>108</sup> Even if systems work as intended, schools may not have individuals trained in interpreting and applying the results of data analysis.<sup>109</sup> There are ethical implications when students and parents cannot, in practice, consent, or opt-out of participation in these experiments. Technology providers, educators, and researchers also conduct what are essentially experiments on students when testing out different innovations.<sup>110</sup> They rarely obtain explicit consent to such experimentation or undergo

---

doubt-about-early-warning-systems-effect-retention [hereinafter Straumsheim, *Mixed Signals*].

<sup>106</sup> Steve Kolowich, *Are Struggling College Students Like Cuddly Bunnies That Should Be Drowned?*, THE CHRON. OF HIGHER ED. (Feb. 12, 2016), <http://chronicle.com/article/Are-Struggling-College/235311?cid=cp30>.

<sup>107</sup> See, e.g., Singer, *Deciding*, supra note 47; Stephanie Simon, *Big Brother: Meet the Parents*, POLITICO (June 8, 2014, 4:58 PM), <http://www.politico.com/story/2014/06/internet-data-mining-children-107461>.

<sup>108</sup> See, e.g., Straumsheim, *Mixed Signals*, supra note 105.

<sup>109</sup> See Milford McGuirt, David Gagnon, & Rosemary Meyer, *Embracing Innovation: 2015–2016 Higher Education Industry Outlook Survey*, KPMG (Nov. 4, 2015), <http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2015/he-outlook-2016.pdf>.

<sup>110</sup> Barbara Means & Kea Anderson, *Expanding Evidence Approaches for Learning in a Digital World.*, OFF. OF EDUC. TECH., U.S. DEPT. OF EDUC. (2013) (“A/B testing can compare alternative versions of a Web-based product with thousands of users in a short time period, leading to insights as to whether alternative A or alternative B is more promising.”).

Institutional Review Board scrutiny. These experiments nevertheless may have a significant impact on learning outcomes.<sup>111</sup> Most schools do not have guidelines in places that take into account how experimental innovation designed to benefit future generations or the broader education system might harm today's student data subjects.

#### D. Neglects the Pedagogical Effects of Data-Driven Education

##### 1. PERVASIVE SURVEILLANCE

Ubiquitous collection of student information may have pedagogical effects that discourage the intellectual exploration and risk-taking traditionally valued in learning spaces. Intellectual privacy is "essential to the First Amendment values of free thought and expression."<sup>112</sup> Students are increasingly exposed as they study online and are confronted by the all-pervasive gaze of public institutions.<sup>113</sup> Legal doctrine and social science both recognize the importance of surveillance effects that occur when subjects are aware that their activities are being monitored.<sup>114</sup> Chilling effects occur when subjects are aware that they are being observed and become self-conscious, thus circumscribing their activities accordingly.<sup>115</sup> This often results in less experimental behavior and may reduce participation and expression overall. Conforming effects occur when students aware of being under observation change their viewpoints to reflect what they consider to be mainstream opinion.<sup>116</sup> These behavioral changes are

---

<sup>111</sup> See Carl Straumsheim, *Study Finds Inconclusive Results About Efficacy of Adaptive Learning*, INSIDE HIGHER ED. (Jun. 23, 2016, 3:00 AM), <https://www.insidehighered.com/news/2016/06/23/study-finds-inconclusive-results-about-efficacy-adaptive-learning>.

<sup>112</sup> Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

<sup>113</sup> See generally Dan Knox, *A Good Horse Runs at the Shadow of the Whip: Surveillance and Organizational Trust in Online Learning Environments*, 7 CAN. J. MEDIA STUD. 1 (June 2010), <http://cjms.fims.uwo.ca/issues/07-01/dKnoxA-GoodHorseFinal.pdf>.

<sup>114</sup> See Frank Pasquale & Danielle Keats Citron, *Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society*, 89 WASH. L. REV. 1413, 1418 (2014).

<sup>115</sup> See Richards, *supra* note 112, at 403.

<sup>116</sup> See Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 502 (2015).



pernicious in part because they can occur without consciousness awareness.<sup>117</sup>

Information practices that encourage conformist opinions cut against traditionally accepted educational goals such as providing a full marketplace of ideas, encouraging critical thinking, and promoting a populace tolerant of diverse viewpoints.<sup>118</sup> Constant surveillance, for example, “undermines the free development of personality upon which free expression depends.”<sup>119</sup> Constant monitoring may normalize surveillance as the default state of being for the next generation of students.

## 2. EMBEDDED ASSESSMENT

These new learning tools, assessment affordances, and competency-based credentialing systems make it possible for real time modeling and analysis of student performance.<sup>120</sup> Most education technology tools offer teachers data visualizations diagnosing student progress to facilitate differentiation of instruction.<sup>121</sup> This may create more accurate representations of a student’s abilities than one-time, high-stakes tests. As one researcher notes:

As opposed to the physical classroom, there is a virtual record of every transaction that takes place in the classroom. Every discussion post, every essay, every teacher comment is captured for posterity. In hun-

---

<sup>117</sup> See *id.* at 512–14 (“Through a desire to publicly conform, they may chose [*sic*] not to express their conflicting views, and through cognitive dissonance, they may gradually be led to believe the majority viewpoint.”).

<sup>118</sup> See *id.* at 511–14.

<sup>119</sup> See Pasquale & Citron, *supra* note 114, at 1419.

<sup>120</sup> See Łukasz Kidziński et al., *A Tutorial on Machine Learning in Educational Science*, in STATE-OF-THE-ART AND FUTURE DIRECTIONS OF SMART LEARNING 453 (Yanyan Li et al. eds., 2016); YANYAN LI ET AL., STATE-OF-THE-ART AND FUTURE DIRECTIONS OF SMART LEARNING (2016); see also Peter Mikuļecky, *Decision Processes in Smart Learning Environments*, in COMPUTATIONAL COLLECTIVE INTELLIGENCE 364 (Ngoc Thanh Nguyen, Lazaros Iliadis, Yannis Manolopoulos & Bogdan Trawinski eds., 2016); SMART LEARNING ENVIRONMENTS (Maiga Chang & Yanyan Li eds., 2015).

<sup>121</sup> Sandra Nam, *Making Learning Easy by Design: How Google’s Primer Team Approached UX*, MEDIUM (Oct. 13, 2015), <https://medium.com/google-design/designing-a-ux-for-learning-ebed4fa0a798>.

dreds of thousands of classes there is data being captured that can be analyzed and sorted. This means that for the first time there is a map of what happens in the classroom. Big Brother can now see everything.<sup>122</sup>

These programs not only see, but memorialize, “everything.” Many educators want to take advantage of the ability to create highly granular data representations of a student’s performance to circumvent the problems of high-stakes and standardized testing.<sup>123</sup> Some reformers suggest using computerized programs to determine proficiency and award “credit” for specific skills. Instead of transcripts, students would have digital records that display their algorithmically-determined competencies.<sup>124</sup> This means that every bit of data captured as students learn—and make mistakes—can be incorporated into the information that will serve as the key to future opportunities.

This ability of educational tools to embed assessments into everyday teaching has important implications on the intellectual privacy and safety of learning environments.<sup>125</sup> Using real-time automated assessments as markers of progress and proficiency collapses the separation between teacher feedback, tests, and transcripts.<sup>126</sup> This may raise, not lower, the stakes of student performance in classrooms.

---

<sup>122</sup> Frank B. McCluskey & Melanie L. Winter, *Academic Freedom in the Digital Age*, 22 ON THE HORIZON 136, 142 (2014).

<sup>123</sup> See Natasha Singer, *Privacy Concerns for ClassDojo and Other Tracking Apps for Schoolchildren*, THE 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> [hereinafter Singer, *Privacy Concerns*]; *About*, EDMODO, <https://www.edmodo.com/about> (last visited Feb. 12, 2017).

<sup>124</sup> Jeffrey R. Young, *The New Transcript*, THE CHRON. OF HIGHER ED. (Feb. 29, 2016), <http://chronicle.com/article/The-New-Transcript/235450> (last visited Jun 23, 2016).

<sup>125</sup> See, e.g., Zeide, *Student Privacy*, *supra* note 1, at 353–54; Paul Prinsloo & Sharon Slade, *Student Vulnerability, Agency and Learning Analytics: An Exploration*, 3 J. OF LEARNING ANALYTICS 159–182 (2016).

<sup>126</sup> See Zeide, *Student Privacy*, *supra* note 1, at 351–55 (reflecting the various ways in which data is collected seamlessly).

Psychological safety is particularly crucial in education.<sup>127</sup> Students take risks and fail frequently in the course of acquiring knowledge and skills,<sup>128</sup> and learning requires vulnerability.<sup>129</sup> Trust, particularly, “has been shown to be a critical affective component of education, impacting the quality of dialogue, academic achievement, and intellectual risk-taking.”<sup>130</sup>

### 3. PERMANENT RECORDS

“Permanent record” fears now apply within education settings as schools increasingly rely on data-driven decisionmaking and retain detailed student information indefinitely.<sup>131</sup> This could create a literal permanent record, one that can be incredibly detailed and widely available.<sup>132</sup>

While long-term retention may ease administrative burdens and facilitate new credentialing, it also cuts against the norms that early mistakes should not foreclose future opportunities.<sup>133</sup> For example, we seal juvenile judicial records.<sup>134</sup> There is a danger that durable data will inaccurately represent students as time moves forward.<sup>135</sup>

---

<sup>127</sup> See Zeide, *Student Privacy*, *supra* note 1, at 352; see also Prinsloo & Slade, *supra* note 125, at 159–182; GERT BIESTA, *BEAUTIFUL RISK OF EDUCATION* (2014).

<sup>127</sup> See Zeide, *Student Privacy*, *supra* note 1, at 390. See also H.R. 1423, 70th Gen. Assemb., 2d Reg. Sess. (Colo. 2016)

<sup>128</sup> See ELIZABETH LOSH, *THE WAR ON LEARNING: GAINING GROUND IN THE DIGITAL UNIVERSITY* 147 (2014).

<sup>129</sup> See *id.*; George Siemens, *The Vulnerability of Learning*, *ELEARNSPACE* (Jan. 13, 2014, 1:17 PM), <http://www.elearnspace.org/blog/2014/01/13/the-vulnerability-of-learning/>.

<sup>130</sup> Knox, *supra* note 113, at 9.

<sup>131</sup> See *Big Data At School: Customising Education or Creating a Permanent Record?*, *THE ECONOMIST* (April 16, 2014) (download using iTunes); Elana Zeide, *The Proverbial “Permanent Record”* 2 (N.Y. Univ. Info. Law Inst., Oct. 2014), [http://www.law.nyu.edu/sites/default/files/upload\\_documents/ProverbialPermanentRecord2014\\_1.pdf](http://www.law.nyu.edu/sites/default/files/upload_documents/ProverbialPermanentRecord2014_1.pdf) [hereinafter Zeide, *Permanent Record*].

<sup>132</sup> See *id.*

<sup>133</sup> See, e.g., Andrew Tutt, *The Revisability Principle*, 66 *HASTINGS L.J.* 1113, 1135 (2015).

<sup>134</sup> See David E. Pozen, *Deep Secrecy*, 62 *STAN. L. REV.* 257, 287 (2010) (“[M]any would agree that it is good for democracy to keep certain juvenile records under seal so that low-level offenders have a chance to enter adulthood without social taint.”).

<sup>135</sup> See Zeide, *Student Privacy*, *supra* note 1, at 354.

This may be more prevalent in students from underserved communities who may require more time and help acclimating to new educational environments and materials.<sup>136</sup> While reformers hope to establish systems that give students control over who can access what portions of their records,<sup>137</sup> it is likely that most will be coerced into full disclosure since those who do not may be judged as having something to hide.<sup>138</sup>

*E. Discounts How Data-Driven Education Technology Shapes Education Itself*

New education technologies do not merely change the medium of education, they shift decisions about the content, metrics, and goals of learning from teachers and administrators to computerized algorithms. These technologies alter the authority and methodology of decisions about instructional content, student assessment, and learning outcomes.

Reformers and researchers are particularly excited by the ability to measure student learning more precisely through data-driven assessment.<sup>139</sup> Big data analytics can create “knowledge maps” that correspond to a rubric of knowledge and concepts.<sup>140</sup> As one education researcher notes:

In the digital classroom, we have a record of where the student interaction was heavy and where student responses were lacking. We can see where student questions arise and where the material seems clear. We can see where the teacher must intervene. We can see patterns of confusion, enthusiasm, and understanding. We can map it as we would a weather pattern or storm. We can find and analyze patterns of faculty interaction, encouragement, and analysis . . . projects underway that compare hundreds of thousands of records to see where activity rise and

---

<sup>136</sup> *See id.*

<sup>137</sup> *See id.* at 356.

<sup>138</sup> *See id.*

<sup>139</sup> *See* LARRY JOHNSON ET AL., THE NEW MEDIA CONSORTIUM, NMC HORIZON REPORT: 2016 HIGHER EDUCATION EDITION 16–17 (2016).

<sup>140</sup> *See* Ayse Saliha Sunar et al., *Personalisation of MOOCs: The State of the Art*, SCI. & TECH. PUBLICATIONS 88, 93 (2015).

fall in online classes. We can now discover patterns that before may have seemed hidden.<sup>141</sup>

This data can then be used to determine what content a platform should present to a student next; to change images on a teacher's dashboard to indicate that a pupil has answered something incorrectly or is taking longer than expected to answer the question; or to act as an embedded assessment that provides evidence that a student has mastered a particular subject or skill.<sup>142</sup> New adaptive platforms increasingly go a step further and automatically adjust instruction and guidance without educator assistance.<sup>143</sup> The most sophisticated of these provide "personalized learning" at scale by altering the content, sequences, and pace of material and assessment in real-time by analyzing embedded assessments using predictive models to better accommodate individual students' needs.<sup>144</sup>

New education technologies do not merely change the medium of education, they shift decisions about the content, metrics, and goals of learning from teachers and administrators to computerized algorithms. Data-reliant technology shapes the benchmarks that educators and institutions track. This, in turn, shapes the learning outcomes they seek to achieve and the goals they pose for students and themselves.<sup>145</sup> Technologies, rather than teachers, end up defining education's purposes.

---

<sup>141</sup> McCluskey & Winter, *supra* note 122, at 142.

<sup>142</sup> Zinaida K. Avdeeva et al., *Smart Educational Environment as a Platform for Individualized Learning Adjusted to Student's Cultural-Cognitive Profile*, in 41 SMART EDUCATION AND SMART E-LEARNING 219 (Vladimir L. Uskov et al. eds., 2015); Vytautas Štuikys, *Robot-Based Smart Educational Environments to Teach CS: A Case Study*, in SMART LEARNING OBJECTS FOR SMART EDUCATION IN COMPUTER SCIENCE 265 (2015); Jinbao Zhang et al., *Smart Learning Environments in School: Design Principles and Case Studies*, in LEARNING, DESIGN, AND TECHNOLOGY 1 (Michael J Spector et al. eds., 2016).

<sup>143</sup> Blanka Klimova, *Teacher's Role in a Smart Learning Environment—A Review Study*, in 59 SMART EDUCATION AND E-LEARNING 2016 51 (Vladimir L. Uskov et al. eds., 2016); *see also* Blanka Klimova, *Assessment in Smart Learning Environment—A Case Study Approach*, in SMART EDUCATION AND SMART E-LEARNING 15 (2015).

<sup>144</sup> *Id.*

<sup>145</sup> *See* Alife Kohn, *Four Reasons to Worry About "Personalized Learning,"* ALFIE KOHN BLOG (Feb. 23, 2015), <http://www.alfiekohn.org/blogs/personalized/>; CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

Representing knowledge and student process in computable terms is necessarily reductive. These epistemologies are not reflections of an objective reality, but constructed frameworks.<sup>146</sup> What can be captured and what is measured shapes the learning outcomes teachers and students aim for. This may skew goal setting towards easily quantifiable factors.<sup>147</sup> Instead of the highly contextualized information available in person, computers can only incorporate the kind of data that can be rendered into a computable format.

More data may not mean more accurate results if data sets are incomplete or too narrowly focused to provide a holistic representation of student progress.<sup>148</sup> Assessments based on algorithmic and automated processing computation have both beneficial and problematic aspects. On the one hand, they could lead to more consistent outcomes than decisions made by humans with more discretion. This may reduce some biased decision-making that currently exacerbates existing socioeconomic inequalities.<sup>149</sup> On the other hand, scholars have consistently demonstrated that big data decision-making can be just as biased as humans or result in disparate outcomes despite seemingly neutral technology.<sup>150</sup>

---

<sup>146</sup> See Wendy Nelson Espeland & Mitchell L. Stevens, *A Sociology of Quantification*, 49 EUR. J. SOC. 401, 408 (2008); Wendy Nelson Espeland & Mitchell L. Stevens, *Commensuration as a Social Process*, 24 ANN. REV. SOC. 313, 326 (1998).

<sup>147</sup> See Kohn, *supra* note 145; O'NEIL, *supra* note 145.

<sup>148</sup> *Id.*

<sup>149</sup> Joshua New, *It's Humans, Not Algorithms, That Have a Bias Problem*, CTR. FOR DATA INNOVATION (Nov. 16, 2015), <https://www.datainnovation.org/2015/11/its-humans-not-algorithms-that-have-a-bias-problem/>.

<sup>150</sup> See Aaron Rieke, *As Schools Mine Students' Data, Longstanding Biases May Gain New Bite*, EQUALFUTURE (Nov. 13, 2013), <https://www.equalfuture.us/2013/11/13/school-data-mining/>; Lauren Kirchner, *When Discrimination is Baked Into Algorithms*, THE ATLANTIC (Sept. 6, 2015), <https://www.theatlantic.com/business/archive/2015/09/discrimination-algorithms-disparate-impact/403969/>; Kate Crawford, *The Hidden Biases in Big Data*, HARVARD BUS. REV. (April 1, 2013), <https://hbr.org/2013/04/the-hidden-biases-in-big-data>.

## V. PATHS FORWARD: ETHICAL QUESTIONS AND NORMATIVE PRINCIPLES

When legislators have included educational purpose clauses in laws, the concern they are likely attempting to address is that a third party might otherwise use the data it collects to disadvantage students (such as through ads or other third party advantage granted by their access to educational data). Given the diversity of legitimate uses for student data and the difficulty of limiting those uses through legal methods alone, it is worth reconceptualizing educational purpose through a combination of legal, normative and ethical frameworks.

Educator communities—particularly in higher education—have begun to promulgate ethical principles to guide student data use.<sup>151</sup> Drawing on the 1973 Code of Fair Information Practices and the Belmont Report of 1979, academic leaders in higher education gathered at the Asilomar Convention for Learning Research in Higher Education and promulgated six principles to inform the storage, collection, analysis, and distribution of data derived from human interaction with learning resources.<sup>152</sup> Organizations in the United

---

<sup>151</sup> See Simon, *Big Biz*, *supra* note 47. See generally Elana Zeide, *Parsing Student Privacy: Creating a Parent-Focused Framework for Conversation*, TECH. ACAD. POL'Y (Sept. 18, 2015), <http://www.techpolicy.com/Blog/Featured-Blog-Post/Parsing-Student-Privacy.aspx> [hereinafter, Zeide, *Parsing Student Privacy*].

<sup>152</sup> These consist of: Respect for the rights and dignity of learners; beneficence; justice; openness; the humanity of learning; and continuous consideration. See Convention Document, *The Asilomar Convention for Learning Research in Higher Education 1–2* (June 13, 2014), <http://asilomar-highered.info/asilomar-convention-20140612.pdf> [hereinafter *Asilomar Convention*].

Kingdom<sup>153</sup> and Europe<sup>154</sup> have promulgated their own principles for learning analytics. These principles emphasize traditional privacy notions like confidentiality, security, transparency, informed consent, and access and ability to amend student records.<sup>155</sup> They go further than current purpose limitation regulation, however, arguing for normative and ethical principles as well as procedural

---

<sup>153</sup> See, e.g., *Policy on Ethical Use of Student Data for Learning Analytics Policy*, THE OPEN U. (Sept. 2014), <http://www.open.ac.uk/students/charter/sites/www.open.ac.uk.students.charter/files/files/ecms/web-content/ethical-use-of-student-data-policy.pdf>. The Open University set forth eight principles for ethical use of student data for learning analytics. See *id.* at 6. These highlight the need for educational data practices to align with organizational principles; use data for the benefit of students; not define students solely by visible data; have well-defined purposes and boundaries; be transparent, accessible, and amendable by students; engage students as active agents; be processes and employed without bias; and through appropriately skilled actors. See *id.* Principle 6 includes informed consent, personalized learning paths, and interventions as examples of how students can be active agents in the implementation of learning analytics. See *id.* A code of practice developed by the Joint Information Systems Committee (JISC) focuses on ensuring responsibility, transparency and consent, privacy, validity, access, positive interventions, minimizing adverse effects, and data stewardship. See generally Niall Sclater & Paul Bailey, *Code of Practice for Learning Analytics*, JISC (June 2015), [http://www.jisc.ac.uk/sites/default/files/jd0040\\_code\\_of\\_practice\\_forlearninganalytics190515v1.pdf](http://www.jisc.ac.uk/sites/default/files/jd0040_code_of_practice_forlearninganalytics190515v1.pdf).

<sup>154</sup> Hendrik Drachsler & Wolfgang Greller, *Privacy and Analytics – It's a DELICATE Issue: A Checklist for Trusted Learning Analytics in 6TH INT'L CONF. LEARNING ANALYTICS & KNOWLEDGE* 89–90 (Apr. 25, 2016), <http://dl.acm.org/citation.cfm?doid=2883851.2883893> (follow “Full Text: PDF” hyperlink). The European Learning Analytics Community Exchange (“LACE”) has developed a checklist of eight points echoing the same ethical themes: determining the purposes served by using student data, defining the scope of collection and use, explain legal compliance, involve stakeholders, seek consent, maximize anonymization, monitor data access, and ensure data recipients have high security standards. See *id.* at 96.

<sup>155</sup> See Asilomar Convention, *supra* note 152, at 2 (“Respect for the rights and dignity of learners[:] Data collection, retention, use, and sharing practices must be made transparent to learners, and findings made publicly available, with essential protections for the privacy of individuals. Respect for the rights and dignity of learners requires responsible governance by institutional repositories and users of learner data to ensure security, integrity, and accountability. Researchers and institutions should be especially vigilant with regard to the collection and use of identifiable learner data, including considerations of the appropriate form and degree of consent.”).



and technical reform.

These manifestos highlight the importance of education actors using data in a deliberate and thoughtful manner.<sup>156</sup> In doing so, they point toward possible ways forward for student privacy protection, whether implemented on an institutional, industry, or regulatory level. They propose both procedural checks on information practices and promote specific normative principles.<sup>157</sup> They emphasize the need to support both learners and institutional growth, as well as scientific inquiry.<sup>158</sup> Educators call upon their own institutions to act as act as fiduciaries for student data.<sup>159</sup> These actors advocate for institutions to employ student data and learning analytics to serve defined purposes, in ways that benefit students, and only as one of many ways to assess a students.<sup>160</sup> They also exhort educators to be mindful of employing data to ameliorate inequalities in learning opportunity and educational attainment, as well as ensuring just distribution of benefits and harms.<sup>161</sup>

Resolving these tensions requires not only technological and procedural compliance, but also engaging normative and ethical considerations. Doing so in any standardized fashion is difficult given the diversity of students, educators, and institutions in the American system. General principles may be articulated to guide in-

---

<sup>156</sup> See Zeide, *Student Privacy*, *supra* note 1, at 340; See NASBE, *supra* note 80, at 13.

<sup>157</sup> See *id.*

<sup>158</sup> See Polonetsky & Tene, *Who Is*, *supra* note 1, at 932–33, 953–54. See generally Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584(a)–(e) (West 2015); Polonetsky & Jerome, *Student Data*, *supra* note 88; Leong, *supra* note 77.

<sup>158</sup> SOPIPA prohibits operators from using, selling, disclosing, and engaging in targeted marketing with K-12 student data. See CAL. BUS. & PROF. CODE § 22584(a)–(b).

<sup>158</sup> H.R. 1423, 70th Gen. Assemb., 2d Reg. Sess. (Colo. 2016).

<sup>158</sup> See Zeide, *Student Privacy*, *supra* note 1, at 370–71.

<sup>159</sup> See *id.*

<sup>160</sup> See Asilomar Convention, *supra* note 152, at 1.

<sup>161</sup> See *id.* (“Justice[:] Research practices and policies should enable the use of learning data in the service of providing benefit for all learners. More specifically, research practices and policies should enable the use of learning data in the service of reducing inequalities in learning opportunity and educational attainment.”).

quiry, but fine-tuning is likely to require highly contextualized decisions based on community or societal norms, student attitudes, and institutional goals.<sup>162</sup>

#### CONCLUSION

New education technology and school information practices undermine the efficacy of traditional student privacy protections that govern access to education records. Reforms relying on education purpose limitations help address concerns about commercial use; but they, themselves, rest on outdated assumptions about today's information technology. They provide predominantly technical and procedural requirements on school data use.

Doing so neglects the reality that schools' use of student data in the service of educational purposes has its own problematic aspects. Issues regarding educational use of student information will become more prominent as data-driven and data-reliant services become integral to students' educational experience. As algorithmic and automated tools increasingly define the content, metrics, and goals of instruction, our educators, technologists, and policymakers must account for the pedagogical impact of shifting from human to computerized decisionmaking. This requires explicit consideration of normative considerations and ethical questions. We will need to continue to define, and re-define, student privacy in light of the kind of education we seek to create and the outcomes we wish to promote.

---

<sup>162</sup> See Zeide, *Student Privacy*, *supra* note 1, at 345.