The Proverbial "Permanent Record"

Elana Zeide, M.F.A., J.D., LL.M.

Research Fellow
Information Law Institute
New York University School of Law

October 2014

The Proverbial "Permanent Record"

By Elana Zeide[1]

The debate about student privacy is highly emotional and divisive. Students, parents, and stakeholders worry about what types of information schools, educational agencies, and third parties collect; who can access it; what it can be used for; and how it remains secure. One prominent fear is that current and proposed information practices have created a proverbial "permanent record" that will tether students to their pasts and limit opportunities later in life. In popular imagination, a stern principal warns a student that his misdeeds will be recorded in his permanent record unless he behaves better.

Permanent record fears fueled the backlash that brought down inBloom, a nonprofit data repository designed to store states' comprehensive student records.[2] Stakeholders express similar concerns regarding the creation of state longitudinal data systems (SLDSs) that link student information over time.[3] Media portrayals of state systems fuel these anxieties by projecting aspects of the imaginary permanent record onto current practices. This discussion points to important places where current information practices conflict with traditional expectations about information flow in public education. However, it also reflects a considerable amount of conflation and misinformation about current practices regarding state creation of longitudinal data systems.

Public education institutions and agencies have not created a "permanent record" where individuals can access students' educational histories at a keystroke. Critiques of state data collection based on this myth suggest—inaccurately—that states collect sensitive student information in a consolidated database that is freely shared with entities like college admission boards, employers, and corporate profiteers. This confusion distracts stakeholders and inhibits the implementation of reforms to ensure appropriate practices regarding student information.

This paper examines the concerns captured in the concept of the proverbial "permanent record," how closely these fears match and diverge from information flow surrounding SLDSs, and the ways that address these fears. It notes where permanent record concerns point to issues that have yet to be addressed by policymakers, and it suggests mechanisms to clarify the debate and better address stakeholder fears by providing a privacy infrastructure and baseline substantive protections.
Fears surrounding the mythical permanent record are only partly about "permanence" or "recording." They also incorporate the sensitivity of information collected about students, the scope

[1] Elana Zeide is an attorney and research fellow at New York University's Information Law Institute.
[2] Omer Tene, *InBloom Wilts Amid Privacy Backlash,* PRIVACY PERSPECTIVES (April 22, 2014), https://www.privacyassociation.org/privacy_perspectives/post/inbloom_wilts_amid_privacy_backlash; Olga Kharif, *Privacy Fears Over Student Data Tracking Lead to InBloom's Shutdown*, BUSINESSWEEK (May 1, 2014), http://www.businessweek.com/articles/2014-05-01/inbloom-shuts-down-amid-privacy-fears-over-student-data-tracking.
[3] David Sirota, *Big Data Means Kids' "Permanent Records" Might Never Be Erased*, MOTHERBOARD (October 24, 2013), http://motherboard.vice.com/blog/permanent-records-are-hurting-kids.

of actors who can access it, and the propriety of using information generated in educational environments to drive decontextualized decisionmaking. Current legal, technological, and administrative measures address these concerns in part by de-identifying student information, segregating data systems, and limiting the disclosure of personally identifiable information (PII) to authorized recipients for specific purposes. These include legislation like the Family Educational Rights and Privacy Act (FERPA), as well as data system architecture and governance protocols implemented by state educational agencies (SEAs) and their third-party service providers. This framework gives educational institutions and agencies the responsibility to establish appropriate data governance and make substantive decisions regarding student information.

However, new information practices unsettle stakeholder trust in these mechanisms. Cloud computing raises questions about data security and the risk of unauthorized access. Third parties increasingly provide educational actors with information management services. Big data analytical techniques complicate traditional notions of what makes a particular piece of information sensitive and what constitutes an educational purpose. Policymakers need to focus on the concerns embodied in the proverbial permanent record with a clear understanding of actual information practices to be able to provide responsive reforms. Towards that end, this paper recommends states create comprehensive data inventories, increase transparency about data practices, provide baseline privacy infrastructure, and ensure the accountability of both public and private actors.

The Shifting Student Information Landscape

Fears about the collection of cumulative records about students are not new, but new and newly visible information practices intensify these concerns. Student data have been digitized for at least a decade, but they were not detailed or accessible enough to provide educators with comprehensive insights about student progress.[4] The information available is frequently stored in incompatible datasets developed for specific applications.[5]

Recent technological advances, like cloud computing, have made storing, linking, transferring, and analyzing large amounts of information easier and less expensive.[6] Student information is now not only digitized, but "datafied"—recorded, stored, and organized in a format that is portable, searchable, and computationally manipulable.[7] Datafication creates extraordinary functionality by allowing data users to aggregate information from numerous sources, analyze it, and use it to make more informed decisions about policy administration and instructional policies.[8]

---

[4] Bill Fitzgerald, *Data Collection Isn't New. And It Predates Common Core*, FUNNYMONKEY (January 6, 2014), http://funnymonkey.com/blog/data-collection-isnt-new-and-it-predates-common-core.
[5] Ryan Baker & George Siemens, *Educational data mining and learning analytics*, CAMBRIDGE HANDBOOK OF THE LEARNING SCIENCES (2014), http://www.ebooksmagz.com/pdf/educational-data-mining-and-learning-analytics-columbia-university-170268.pdf.
[6] Nabil Sultan, *Cloud computing for education: A new dawn?* 30 International Journal of Information Management 109 (2010).
[7] *See* Katherine J. Strandburg, *Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context*, in PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT (2014).
[8] National Center for Education Statistics, *Statewide Longitudinal Data Systems Grant Program*, http://nces.ed.gov/programs/slds/resources.asp. This funding incorporates grants related to several different statutes, including the Statewide Longitudinal Data Systems grant program, the American Recovery and Reinvestment Act, and Race

State Longitudinal Data Systems

Educators, schools, and educational agencies increasingly turn to data to evaluate educators, institutions, instructional design, pedagogical methodology, curricula, and technological applications.[9] By analyzing students' success over time, schools have more precise ways "to determine what works, identify ways to improve instruction, tailor approaches to individual students, recognize problems early on to prevent academic failure and dropouts, and automate and streamline daily administrative operations."[10]

Over the past 10 years, the federal government has provided funds for states to create longitudinal information systems that link information about students over time.[11] These systems improve information interoperability, allowing different software systems to share data through common data standards and definitions. They also improve portability, so that information can move between systems.[12] Longitudinal data systems store and maintain student- and staff-level and aggregate data, link data across entities and time, and make data accessible through reporting and analysis tools at various degrees of detail and comprehensiveness.

These efforts originated at the K–12 level, but are expanding in scope. P–20/workforce (P–20W) data systems link information about students that ranges from prekindergarten through entry into the workforce to provide a more comprehensive picture about how students' perform over time.[13] By matching P–12 and postsecondary information, educators can examine the relationship between a student's high school courses, grades, and test scores with their ability to stay in and graduate. By connecting education and workforce data, researchers can analyze whether schools are adequately preparing students for long-term success.[14]

Concerns about the Proverbial Permanent Record

---

to the Top. Most states also provide their own funding. *See* Data Quality Campaign, *Getting the Facts Straight about Education Data*, http://dataqualitycampaign.org/files/Safeguarding%20Data%20-%20Getting%20Facts%20Straight.pdf.

[9] Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, Center on Law and Information Policy (2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip [hereinafter "CLIP Cloud Computing Study"].

[10] National Forum on Education Statistics, TRAVELING THROUGH TIME: THE FORUM GUIDE TO LONGITUDINAL DATA SYSTEMS. BOOK ONE OF FOUR: WHAT IS AN LDS? (2010) at 20.

[11] *Id.* ("An education longitudinal data system is a data system that collects and maintains detailed, high quality, student- and staff-level data that are linked across entities and over time, providing a complete academic and performance history for each student; and makes these data accessible through reporting and analysis tools.") *See also* http://nces.ed.gov/forum/ldsguide/book1/ch_2_1.asp.

[12] National Forum on Education Statistics, TRAVELING THROUGH TIME: THE FORUM GUIDE TO LONGITUDINAL DATA SYSTEMS. BOOK TWO OF FOUR: PLANNING AND DEVELOPING AN LDS, (2010), at 51 [hereinafter "Traveling Through Time 2"].

[13] William A. Sederberg & Barry Stern, *Data: The Link between Higher Education and the Workforce We Need*, (June 2, 2014), http://www.governing.com/gov-institute/voices/col-linking-data-higher-education-workforce-development.html.

[14] *See, e.g.*, Benjamin Herold, *Americans Worried, Uninformed About Student Data Privacy, Survey Finds*, EDUCATION WEEK (January 22, 2014), http://blogs.edweek.org/edweek/DigitalEducation/2014/01/american_worried_uninformed_student_data_privacy.html?cmp=SOC-SHR-FB; Michelle R. Davis & Sean Cavanagh, *Cloud Computing in K-12 Expands, Raising Data Privacy Concerns*, EDUCATION WEEK (January 1, 2014), http://www.edweek.org/ew/articles/2014/01/08/15cloud_ep.h33.html?qs=privacy.

Much of the debate about the creation of P–20W programs conflates information practices involving longitudinal data systems with other educational policy issues. These institutional, pedagogical, and political issues bear serious consideration. However, they are distinct and should be considered separately from issues regarding appropriate information practices within the current regime. It is important to separate information practices from broader issues and distinguish between different users and information practices within and outside the educational system and between educational institutions at various local, state, and federal levels. These include the collection, storage, disclosure, use, and retention of information about or generated by students.

Students, parents, and stakeholders worry about what type of information schools and educational agencies collect, who can access it, what it can be used for, and how it remains secure.[15] The conversation captures prevalent concerns about the consequences of collecting and retaining previously ephemeral student information, the risks posed by consolidating student data, and the use and repurposing of information to serve noneducational or commercial interest. There is also considerable confusion about current information practices due to a lack of transparency and the complexity of institutional, technological, and legal frameworks governing student information. We need to be wary of projecting remnants of the proverbial permanent record onto current information practices.

As Viktor Mayer-Schonberg and Kenneth Cukier provocatively put it, "Your High School Transcript Could Haunt You Forever."[16] Parents and privacy advocates worry that students' early behavior and performance will follow them through the educational system and into the workplace, where decisions will be based on outdated or irrelevant information.[17] They wonder if "a data point could be the difference between a college acceptance letter and a rejection letter?"[18] They fear that disclosure of sensitive information will harm a student's reputation and unfairly foreclose future opportunities.[19]

Notably, the anxieties captured in the proverbial permanent record are only partly about "permanence." They are not as much about the longevity of record keeping as the content of information collected about students, the scope of actors who can access it, and the propriety of decontextualized decisionmaking. These combine to create a fear that unauthorized actors will obtain and judge students unfairly based on outdated, inaccurate, or inappropriate information.

Longevity

---

[15] *See, e.g.,* Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (October 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?_r=0.
[16] Viktor Mayer-Schönberger & Kenneth Cukier, *Your High School Transcript Could Haunt You Forever*, THE ATLANTIC (March 11, 2014), http://www.theatlantic.com/education/archive/2014/03/your-high-school-transcript-could-haunt-you-forever/284346/.
[17] Sirota, *supra* note 3.
[18] *Id.*
[19] *Id.*; Anya Kamenetz, *What Parents Need To Know About Big Data And Student Privacy,* NPR (April 28, 2014), http://www.npr.org/blogs/alltechconsidered/2014/04/28/305715935/what-parents-need-to-know-about-big-data-and-student-privacy.

The fact that we have the concept of a permanent record is telling in and of itself. It implies that there are impermanent records as well—and that student information is by default not "permanent." If recording information in a permanent record were routine, it would not bear mention, let alone be used as a threat or punishment. Instead, recording information in an imaginary permanent record works as a threat because it is an atypical occurrence. This corresponds with the traditional evaluation model in the United States where informal assessment over the course of instruction is typically used as feedback and to inform immediate pedagogical decisions. In contrast, the recording of summative, end-of-semester grades is the norm.[20]

In and of itself, the longevity of stored information about students is not the cause of the degree of concern that has developed about information practices in education. Schools have retained transcript-level information about students indefinitely. Students have had a permanent record for at least a generation consisting of transcripts with course enrollment, end-of-semester grades, and instructors' names.[21]

Content

The permanent record in the popular imagination has also been conceptualized as a disciplinary tool, which is instructive. It implies that the information collected will be relevant enough to factor into future decisionmaking. It also suggests that this information is sensitive—and probably negative. It is telling that urban dictionaries define the permanent record as "Where all the bad things you've done as a child go."[22] Here, the concept of a permanent record assumes there is no neutral information used for diagnostic and feedback purposes, or positive content like awards and improvement. This contributes to the resistance to longitudinal data systems. In the popular imagination, putting something in a permanent record is punishment, putting students in peril. This makes it difficult for stakeholders to consider recordkeeping as a tool to help them progress.

Disclosure

Concerns about the permanent record also draw from the assumption that the information it contains will be disclosed to outside entities to inform their decisionmaking. The prospect of a permanent record would hold no threat if it did not reveal new information to new recipients.[23]

---

[20] *See, e.g.,* Nick Hytrek, *Permanent student record is just that*, SIOUX CITY JOURNAL (April 30, 2011), http://siouxcityjournal.com/special-section/siouxland_life/permanent-student-record-is-just-that/article_56ff2bfc-cfff-52d9-aed8-46b2fd67aacc.html.

[21] For example, Mississippi's law requiring the creation and maintenance of cumulative and permanent records about students has been in effect since 1954. Mississippi Cumulative Folders and Permanent Records Manual of Directions, (2010), http://www.mde.k12.ms.us/docs/accreditation-library/ms-cumulative-folders-and-permanent-records-manual-1-doc.pdf. Iowa's "permanent records" contain students' names, dates of birth, gender, ethnicity, contract information, class enrollment, grades, and credits or credentials earned. Iowa Permanent Record Information, http://www.sai-iowa.org/Legal%20Issues/General%20Legal%20Topics/permanentrecord.pdf.

[22] Urban Dictionary: permanent record, http://www.urbandictionary.com/define.php?term=permanent+record.

[23] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 490 (January 2006) (Disclosure can also be harmful because it makes a person a "prisoner of [her] recorded past.").

Again, social norms regarding student information disclosure vary. Stakeholders expect that employers will use student transcripts in the course of evaluating job applicants, but bridle at the notion of employers being able to access other types of information stored in SLDSs.[24] They also worry that information will be repurposed to serve competing interests within the educational sphere or of third parties.[25]

The permanent record concept also includes the sense of a consolidated, coherent dossier. This corresponds with the traditional notion of records retained in physical files. There is a corresponding notion of all-or-nothing access—anyone with access to the filing cabinet or a single file could peruse information at will without impediment.

Decontextualized decisionmaking

There is also a sense that it is inappropriate for certain information to be factored into decontextualized decisionmaking both for educational and noneducational purposes.[26] Stakeholders and advocates fear that older information will no longer accurately reflect a student, that quantified information cannot be comprehensive, and that atomized information will not be representative.[27]

These fears also reflect concerns that captured information will undercut social values and goals incorporated in the essence of public education in America. We don't hold children to the same standards of accountability or long-term consequences of their early actions.[28] Minors cannot enter into binding contracts and most juvenile detention records are sealed or expunged when a person turns reaches the age of majority. This sense of reinvention, progress, and progression also echoes the social values and goals integral to the public education system in America: the democratic ideals of equality of opportunity, social and economic mobility, and meritocracy.[29]

Protection against the Proverbial Permanent Record

Fears about the proverbial permanent record capture concerns about the collection and retention of sensitive information about students, its disclosure to third parties, and its use to drive decontextualized decisionmaking. SDLSs are understandable targets for concerns because they implicate several aspects of the proverbial permanent record. They collect significant amount of

[24] Emmett McGroarty, Joy Pullmann & Jane Robbins, *Cogs in the Machine: Big Data, Common Core and National Testing* (2014), http://www.stopccssinnys.com/uploads/Cogs_in_the_Machine.pdf; Leonie Haimson, *inBloom testimony*, CLASS SIZE MATTERS (September 30, 2013), http://www.classsizematters.org/wp-content/uploads/2013/09/testimony-re-Bloom-9-30-2013.pdf.
[25] Alex Molnar et al., *Schoolhouse Commercialism Leaves Policymakers Behind*, NATIONAL EDUCATION POLICY CENTER, http://nepc.colorado.edu/publication/schoolhouse-commercialism-2013.
[26] *See* Viktor Mayer-Schönberger & Kenneth Cukier, LEARNING WITH BIG DATA (2014).
[27] *Id.*
[28] *Id.;* Joel Reidenberg et al., *Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems*, (2009), http://papers.ssrn.com/abstract=1495743 [hereinafter "CLIP Children's Privacy Study"].
[29] A full accounting of this is beyond the scope of this paper, but addressed more fully in my forthcoming article, *Student Privacy in Context*.

information, some of which may be considered sensitive, retain it for a long period of time, and explicitly use this information to inform decisionmaking. However, the concept of the proverbial permanent record prompts discussion about student data systems as if they are a monolithic database accessible at a keystroke. Descriptions of information "securely linked" between different data systems morphs into the idea that student information is consolidated into "one easily accessible file."[30]

This does not comport with the current realities of the SLDS. The current framework for SLDSs addresses these concerns by limiting the disclosure of personally identifiable information to authorized third parties who can only use it for approved purposes, must protect against further disclosure, and must destroy the information when no longer needed to serve its purpose. Various regulatory, technological, physical, and administrative structures have been put into place to minimize the potential for unauthorized access to personally identifiable student information. The information contained in SLDSs is segregated in separate databases or data sets, stripped of personally identifiable information or associated with a unique student identifier instead of the student's name. PII cannot be disclosed to third parties without formal authorization. Even among authorized recipients, access to potentially sensitive student information is limited based on particular data users' role and needs.

These mechanisms help protect against concerns about collection, retention, sensitive information, disclosure, and decontextualized decisionmaking embedded in the concept of the permanent record. The degree to which this structure is effective, however, depends on how well educators, administrators, and SEA personnel act within this framework to make authorization, anonymization, purpose specification, and retention meaningful. It also depends on how they supplement the existing framework to cover a sufficiently broad array of potentially sensitive information and create direct consequences for both educational actors and third parties.

Overview of Information Practices

Schools, local educational agencies (LEAs), and SEAs collect a variety of PII about students. They do so to meet federal and state reporting requirements and obtain funding, ensure accountability, foster transparency, and improve student success by better evaluating policies and programs. Schools share some of the information they collect with districts, regional consortia, and SEAs to comply with federal and state reporting and accountability requirements.[31] The type of data collected, and who can access it, is different at each point. It becomes less specific, more likely to be

[30] Early Childhood Data Collaborative, *2013 State of States' Early Childhood Data Systems* (February 2014), http://www.ecedata.org/files/2013%20State%20of%20States'%20Early%20Childhood%20Data%20Systems.pdf.
[31] *See, e.g.,* Interview with Dan Domagala, Chief Information Officer, Colorado Department of Education [hereinafter "Colorado Interview"]; Interview with Bob Swiggum, Georgia Department of Education's Chief Information Officer [hereinafter "Georgia Interview"]; Interview with Ken Wagner, Deputy Commissioner for Curriculum, Assessment, and Educational Technology, New York State Department of Education [hereinafter "New York Interview"]; CLIP Children's Privacy Study, *supra* note 28.
[31] *Id.*

de-identified and aggregated. Individual student data may be used, for example, to calculate state funding, administer state assessments, or authenticate reports to school staff. Aggregate data may include school and district performance calculations, program monitoring and evaluation, school feedback reports, federal reporting, public reporting resources, and standardized test results.

Information collection and practices vary widely depending on each school and district's size, resources, and technological sophistication.[32] Most states delegate day-to-day data security, management, and governance to districts, which store information in student information systems.[33] Information passes from schools to districts, sometimes to regional consortia, on to SEAs and the US Department of Education (ED). States share information with the federal government in aggregate form in compliance with reporting statutes.[34] The federal government is prohibited from creating a national student database.[35] It does not have access to any of the PII in state data systems.

Information Content and Sources

The information available about the data states collect consists predominantly of online lists of elements used in various data systems, making it difficult to get a clear sense of actual information practices.[36] At minimum, however, schools record students' names; birthdates; contact information; demographics; enrollment; coursework; attendance; dropout and graduation rates; state, local, and national assessments; and credentialing.[37] K–12 schools must also collect information about teacher qualifications and students' participation in various special programs like special education, migrant worker status, and free and reduced-price meal programs.[38]

States collect or connect information to create longitudinal data systems.[39] They link this to data from other educational sources like higher education systems.[40] This includes student enrollment, demographic statistics, special program participation, state and college readiness test results, course completion, and dropout or graduation status. States increasingly link this to information about early childhood and workforce programs. This often involves analyzing information from other state

[32] Alicia Solow-Niederman, Leah Plunkett & Urs Gasser, *Student Privacy and Cloud Computing at the District Level: Next Steps and Key Issues*, BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378568; CLIP Cloud Computing Study, *supra* note 9.
[33] *Id.*
[34] *See, e.g.*, Frequently Asked Questions: *CEPI Data Systems Privacy and Security Practices*, (2014), http://www.michigan.gov/documents/cepi/FAQs-SecurityPrivacy_462084_7.pdf [hereinafter "Michigan SLDS FAQ"]; *ANSWERS Frequently Asked Questions – Alaska's P–20WP–20W SLDS*, (2014), http://acpe.alaska.gov/DATA-REPORTS/Partnership_Initiatives/ANSWERS/FAQs [hereinafter "Alaska SLDS FAQ"].
[35] *See generally*, National Center for Education Statistics, *Statewide Longitudinal Data Systems Grant Program*, http://nces.ed.gov/programs/slds/resources.asp.
[36] Dan Abendschein, *Some surprising facts about states and data*, MARKETPLACE.ORG (September 18, 2014), http://www.marketplace.org/topics/education/learningcurve/some-surprising-facts-about-states-and-student-data.
[37] Traveling Through Time 2, *supra* note 12, at 16-18.
[38] *See, e.g.*, http://www.ksde.org/Portals/0/Communications/Publications/Fact%20Sheets/FACT_SHEET_Data_Coll_0913.pdf [hereinafter "Kansas Fact Sheet"]; Michigan SLDS FAQ, *supra* note 34.
[39] Schools, LEAs, and SEAs generally use a web-based interface to provide authorized users with access to datasets reflecting some of this information.
[40] For example, the Kansas Department of Education collects information from the Kansas Board of Regents and National Student Clearinghouse.

agencies' data systems, including employment, social service, and public benefit programs, to evaluate education and workforce programs and provide better services to schools and students.[41] For example, several states publicize average earning for graduates of education and training programs. Kentucky matches state unemployment insurance wage records with student information to provide colleges with aggregate employment outcomes by institution and program. Maine uses a similar program to report aggregate employment rates and earning related to various programs of study.

Generally, states do not collect data about a student's (or his guardians') beliefs about sex, family life, morality, religion, or politics.[42] Nor do they collect political, voting, family financial, biometric, or medical reports, including information on student psychosocial or emotional state.[43] However, schools, districts, and states may choose to collect additional information about students for administrative and evaluative purposes.[44] Some of this information is health-related. Alaska, for example, collects information about students' oral health.[45] Colorado has an element in its data dictionary to indicate if a student is taking a weight reduction supplement.[46] Some schools collect information for disciplinary purposes, some of which may be considered sensitive. For example, when Florida tracks incidences of bullying, it also collects information as to the reason why a student was bullied—in terms of identifiers like religion and sexual orientation.[47]

This type of information is beyond the bounds of what many stakeholders expect within the public education framework. Scholars and advocates have criticized states for collecting too much or inappropriate information.[48] The inBloom database accounted for approximately 400 data points educational entities might consider collecting.[49] Are state data elements, similarly, a list of information that could be collected? Were they collected at some point? Are they currently being collected? Who can see this information? What is it used for? Who is it shared with? Is it stored in longitudinal data systems?

---

[41] *See* Rachel Zinn and Andy Van Kluenen, Workforce Data Quality Campaign, *Making Workforce Data Work,* (January 2014), at 5, http://www.workforcedqc.org/sites/default/files/Resource%20PDF/WDQC%20report.pdf.
[42] *CEPI Privacy and Security Policy*, (2014), I_Privacy_Policy_Notice_364597_7.pdf [hereinafter Michigan SLDS Privacy Policy"].
[43] *Id.*
[44] For more detailed information about individual states, Marketplace.org has created a useful reference that links to state-specific data inventories, available at http://marketplace.org/sites/default/iframes/learningcurve/sldsmenu.html.
[45] Alaska Department of Education Data Mangement Table of Contents, http://education.alaska.gov/tls/assessment/handbookuser2/toc.asp?tocid=392841&details=0&parentid=0.
[46] Colorado Department of Education Data Dictionary, https://cdx.cde.state.co.us/DataDictionary/faces/welcome.jspx;jsessionid=NPmYJfTdHbhTwM31gzWon69Ngrol7vTvsR93qdtTVd9zDRQ2Ynyg!-1000521431?_afrLoop=93299274869051 8&_afrWindowMode=0&_afrWindowId=null.
[47] Florida Department of Education Information Database Requirements, http://www.fldoe.org/eias/dataweb/student_1415.asp#data.
[48] CLIP Children's Privacy Study, *supra* note 28; Khaliah Barnes, *Why a Student Privacy Bill of Rights is So Desperately Needed*, THE WASHINGTON POST (March 6, 2013), http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.
[49] This list was derived from the National Education Data Model (NEDM), a conceptual model of potential data points promulgated by the National Center for Education Statistics, available at http://nces.ed.gov/forum/datamodel/. It does not reflect categories of information that states are collecting or are required to collect.

Overview of Information Protections

Similar fears prompted the enactment of FERPA in 1974.[50] FERPA limits the disclosure of PII to preclude this information from informing decisionmaking.[51] FERPA prohibits federally funded schools from disclosing PII maintained in a student's educational record to third parties without parental consent or, through various exceptions, educator approval.[52] De-identified data may be shared without the consent required by FERPA with any party for any purpose.[53]

As defined in FERPA, PII includes the names of a student and his family members, his address, personal identifiers such as social security number, and indirect identifiers such as date of birth or mother's maiden name.[54] It also includes information falling within a catchall provision that "alone or in combination, is linked or linkable to a specific student" in such a way that it would allow someone in the school community "to identify the student with reasonable certainty."[55] An "education record" is one directly related to a student that is "maintained" by an educational agency or a party acting for the agency or institution.[56] For example, FERPA's restrictions apply to information about a student's final grades, special needs, and disciplinary records.

FERPA does not require consent for schools to release "directory information."[57] These are defined as "information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed," including name, street address, email address, photographs, weight and height of athletes, and degrees and awards received.[58] This information has traditionally been used to create parent contact lists, yearbooks, and student athletic statistics. Parents or eligible students can opt out of the disclosure of directory information.[59]

Anonymization

FERPA uses anonymization to mitigate the sensitivity of information. The concept of the permanent record suggests that the information contained in a "record" is associated with a particular student. Without this connection, information contained in the record could not be used as the basis for detrimental decisionmaking about the individual student. SLDSs incorporate this anonymization

[50] Pub. L. No. 93-380 (1974), codified at 20 U.S.C. § 1232g. The regulations that administer FERPA are incorporated in 34 C.F.R. § 99.
[51] 20 U.S.C. 1232g.
[52] *Id.*; 34 C.F.R § 99.5. Parents provide this consent until a student reaches age 18 or enters a postsecondary educational institution.
[53] 34 CFR § 99.30, 99.31(b)(1).
[54] 20 U.S.C. 1232g.
[55] 20 U.S.C. 1232g(f); 34 C.F.R. 99.3.
[56] *Id.* § 1232g(a)(4)(A); 34 C.F.R. 99.3(b)(i).
[57] *Id.* § 1232g(a)(5)(A)-(B); 34 C.F.R. 99.3(b)(1)-(2).
[58] *Id.*
[59] 20 U.S.C §1232g(a)(5)(B).

mechanism by de-identifying student information and associating it with unique student identifiers. By default, they disclose information in aggregated groups that do not permit identification of individual students.

De-identification

De-identification refers to the process of removing or obscuring PII information from student records. Instead of information being associated with a student's name, it is tied to a meaningless code or string of numbers.[60] Data systems use these "unique student identifiers" to associate information with a particular student instead of personal information like names or social security numbers.[61]

This minimizes the risk of unintended disclosure of the identity of individuals and information about them. Educational entities can then share information associated with a specific student without disclosing personally identifiable information. Students cannot be tracked across different information systems unless an individual can access a separate, strictly controlled dataset that contains the information matching student identification numbers.

Many states use different student identification codes for different systems to prevent the code from becoming an identifier in-and-of-itself. Most districts use different unique identifiers than state agencies.[62] Postsecondary institutions may also use a separate identifier in linking and managing information about the student.[63] States may also use special identification codes for the sole purpose of sharing this information with third parties creating SLDS systems.[64]

Aggregation

Information can also be collected and reported according to group characteristics, creating aggregated data sets that do not contain student-level information.[65] In the context of FERPA, aggregation also connotes that information has been reviewed to see if there are any characteristics shared by only a few students who might be re-identified by someone in their community.[66]

Many stakeholders fear that individual students will be inadvertently exposed in data because they

---

[60] *Data De-identification: An Overview of Basic Terms, at* http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf. While it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify an individual.

[61] *Id;* National Forum on Education Statistics, TRAVELING THROUGH TIME: THE FORUM GUIDE TO LONGITUDINAL DATA SYSTEMS. BOOK THREE OF FOUR: EFFECTIVELY MANAGING LDS DATA, (2010) at 18 [hereinafter "Traveling Through Time 3"]; National Center for Education Statistics, *Unique Identifiers: Beyond K12* (March 2014), http://nces.ed.gov/programs/slds/pdf/UID_brief.pdf.

[62] Colorado Interview; Georgia Interview; New York Interview; State IT State Interview.

[63] *See, e.g.,* Kansas Case Study, *supra* note 31 (Students have one identifier associated with information from early childhood through secondary education, and another associated with information associated with post-secondary records.)

[64] *See, e.g.,* Michigan SLDS Privacy Policy, *supra* note 42.

[65] *Id.*

[66] *Id.*

are among a small set of cases. For example, if there is only one Asian female in the third grade of a particular school, then individuals in the school community may be able to infer information relates to her even though it does not contain any identifying information.[67] FERPA's "catchall" provision requires that data users anticipate and prevent this type of inadvertent disclosure.[68] As a result, districts and states do not release or use statistical methods to obscure information about groups with very small subsets. Colorado's Department of Education, for example, will not publically report information with fewer than sixteen members in a particular subgroup.[69]

Dataset Segregation and Selective Access

The proverbial permanent record implies unlimited access to student information. However, states release only limited information to stakeholders and provide data users with varying levels of access to student information according to their roles, needs, and responsibilities. Longitudinal data systems are not the same thing as a consolidated, centralized dossier. Some states combine information from various sources into a central data repository where they are de-identified to separate PII from other data.[70] Most SLDSs connect information by linking data sets.[71] In Virginia, for example, the state system connects information from various sources upon a user's request and delivers a corresponding data set. It uses a "double de-identification" system where both data sources and the state system use different unique identifiers.[72]

Disclosure to Stakeholders

Parents, educators, administrators, and state agency officials cannot directly access raw data stored in longitudinal data systems.[73] Internal controls limit administrators' access to information unrelated to their role within the educational system.[74] An individual seeking access must obtain authorization to do so, typically on a district or state level, indicating what type of information they can access.[75] States record audit trails to monitor who accesses these data systems.[76]

---

[67] Traveling Through Time 3, *supra* note 62, at 65.
[68] 20 U.S.C. 1232g(f) (Personally identifiable information includes information that would permit "a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.")
[69] Colorado Interview.
[70] Susan T. Gooden, Farrah S. Graham, & Kasey J. Martin, *Bridging the Data Divide: Understanding State Agency and University Research Partnerships within SLDS* (February 6, 2014), at 25, http://www.vlds.virginia.gov/pdfs/VCU.BridgingtheDataDivideReport.020614.Final.pdf.
[71] For example, Texas and Washington use systems where repositories managed by the Higher Education Coordinating Board in Texas and the Education Research and Data Center in Washington perform the matching process and deliver results back to various agencies upon request. *Id.*
[72] *VDOE & the Virginia Longitudinal Data System: Improving Student Outcomes & Protecting Privacy* (May 2, 2013), http://www.doe.virginia.gov/info_management/longitudinal_data_system/vlds_information.pdf.
[73] Colorado Interview; Georgia Interview; New York Interview; State IT State Interview.
[74] *Id.*
[75] *Id.*
[76] *Id.*

Parents only see PII about their own children.[77] This information includes attendance, schedules, meal accounts, report cards, and standards-based reports on student performance. Teachers, administrators, and SEA employees seeking access to SLDS information must obtain authorization to do so, typically on a district or state level, indicating what type of information they can access. Some states provide teachers access to student-level longitudinal data.[78] Others restrict teachers to assessment information related to a specific subject.[79] Educators may be able to view PII about a student's history in the subject they teach, but only aggregate data for other classes in the same school.[80] Superintendents have a broader scope of authorization.[81] Very few individuals in SEAs have access to or can alter longitudinal databases. This is limited to only a handful of individuals at the highest levels who have responsibility for data maintenance and security oversight.[82] States increasingly require staff members to sign annual confidentiality agreements. In North Carolina, for example, all staff members of the North Carolina Department of Public Instruction must to sign a confidentiality agreement annually witnessed by their division director.[83]

Disclosure to Third-Party Service Providers

The permanent record myth suggests that information in a student's record will be disclosed beyond the immediate educational context. Some of the confusion surrounding longitudinal data systems stems from the fact that FERPA has different requirements to allow educational actors to share PII without prior consent in different circumstances. These include the school official exception, the studies exception, and the audit and evaluation exception.[84]

School Official Exception. On a school and district level, the majority of disclosure occurs under FERPA's school official exception. FERPA permits schools and districts to disclose PII to third parties they have determined have a "legitimate educational interest" in the information if they maintain "direct control" and use "reasonable methods" to ensure third parties' information practices protect PII from further or unauthorized disclosure.[85] While ED has released best practices regarding the substance and mechanism for this oversight, FERPA does not require formal designation of school official status, specification of the purposes served by disclosure, or threshold data security and

[77] Colorado Interview; Georgia Interview; New York Interview; State IT State Interview; Traveling Through Time 2, *supra* note 12, at 25.
[78] Data Quality Campaign, *Understanding Teacher Effectiveness*, http://dataqualitycampaign.org/files/DQC%20Teacher%20Access%20Jan31.pdf
[79] *Id.*
[80] *Id*. at 25.
[81] Colorado Interview; Georgia Interview; State IT State Interview; New York Interview.
[82] *Id.*
[83] *NC Common Core Explained*, http://www.dpi.state.nc.us/core-explained/faq/?&print=true.
[84] "School Official" Exception, 20 U.S.C. 1232g and 34 CFR § 99.31(a)(1)(i); the "Studies" Exception, 20 U.S.C. §1232g(b)(1)(F) and §99.31(a)(6); the "Audit and Evaluation" Exception, 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5) and §§99.31(a)(3) and 99.35.
[85] *See* 34 CFR § 99.31(a)(1)(i); 99.35; US Department of Education, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (Feb. 2014), http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf.); The Family Policy Compliance Office, *The Family Educational Rights and Privacy Act Guidance for Reasonable Methods and Written Agreements*, at http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf.

governance mechanisms. A recent study by Fordham's Center on Information Law and Policy suggests that schools and districts disclose information without appropriate, clearly defined safeguards in place.[86] A detailed accounting of these issues is beyond the scope of this paper, but the exception is relevant here because commenters frequently discuss SLDSs as if the same framework applied. SEAs cannot use this exception because it only applies to institutions with enrolled students.[87]

Studies and Audit and Evaluation Exceptions. SEAs instead rely on FERPA's "studies" and "audit and evaluation" exceptions, which are subject to more stringent and specific requirements following recent amendments to FERPA's regulations in 2011.[88] The studies exception applies to permit SEAs to share student PII with researchers. The audit and evaluation exception governs disclosure to third parties that helps states create, manage, and analyze information collected to develop or implement P–20W programs.[89] Under FERPA, states can only share PII with these entities after executing a written agreement authorizing the disclosure, prohibiting data recipients from redisclosing or repurposing the information, and obliging them to destroy the information when it is no longer needed to serve its original purpose.[90]

Entities disclosing information under the studies or audit and evaluation exceptions must do so pursuant to written agreements. The educational institution or agency must formally designate the authorized representative, specify the information to be disclosed, and describe the activity with sufficient specificity to make clear that it comes within an authorized purpose. These designated third parties can only use student data for authorized purposes, must protect the data from further disclosure and other uses, and must destroy the data when no longer needed for the authorized purpose.[91] The contract must contain specific policies and procedures to protect the student data from further disclosure and unauthorized use.[92] This includes requiring that the SEA use "reasonable methods" to ensure "to the greatest extent practicable" the authorized representative uses student data only for authorized evaluation, audit, or other compliance purposes.[93] Third parties are prohibited from sharing PII with anyone outside the state agency who retained them or their institution, or in ways that allow individual students to be identified.[94] These designated third parties sign a written contract agreeing that they will only use student data for authorized purposes, protect the data from further disclosure or other uses, and destroy the data when no longer needed for the authorized purpose.

---

[86] CLIP Cloud Computing Study, *supra* note 9.
[87] 34 C.F.R. § 99.7(a)(1)(iv). The school official exception does not apply to SEAs, which do not have enrolled students, who must instead use the "audit and evaluation" exception to outsource functions to "authorized representatives." *See* LeRoy S. Rooker, Letter to Pennsylvania Department of Education re: Disclosure of Education Records to CDC Grantees -- FERPA Online Library (February 25, 2004), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/pacdc.html.
[88] 34 CFR § 99.31(a)(6); 34 CFR §§ 99.31(a)(3) and 99.35; *see* US Department of Education, *Legislative History of FERPA Provisions*, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html.
[89] 20 U.S.C. § 1232g(b)(1)-(5); 34 CFR § 99.31(a)(6).
[90] *Id.*
[91] 34 CFR §§99.31(a)(3), 99.35.
[92] *Id.* § 99.31(a)(3).
[93] 34 CFR §§99.31(a)(3), 99.35.
[94] *Id.*

Researcher requests for student information undergo a review process, generally by an advisory board.[95] States provide access to specific data their research requires and rarely release student level information to researchers. Even in these cases, the information is assigned unique student identifiers.[96]

Retention Limitations. Before these contractual requirements became effective in 2012, a study suggested that many educational actors retained information indefinitely because they did not have data destruction protocols in place.[97] ED recently released guidelines detailing appropriate methods for data destruction.[98] This guidance notes that retention issues may be complicated with respect to longitudinal data systems designed to track students over long periods of time and suggests a variety of best practices, including setting initial retention limits and reevaluating as systems develop.[99] Some states have created specific rules for student information. For example, New York requires longitudinal data systems to delete identifiable student information eight years after a student graduates from secondary education.[100]

Preempting the Proverbial Permanent Record

Today's SLDS structure does not create a modern day equivalent of the proverbial permanent record. The current student privacy framework limits the disclosure of PII to authorized actors and restricts them from repurposing, redisclosing, or retaining information indefinitely. The degree to which this structure is effective depends, however, on whether educational actors use these requirements to create meaningful constraints on inappropriate information practices. FERPA does not require any particular methods that schools, LEAs, and SEAs must use to provide these protections. ED has recently provided more guidance to clarify these terms and suggest best practices.[101] However, broad, nonbinding best practices may not be sufficient to allay stakeholder fears.

Continuing Concerns

The current student privacy framework only addresses stakeholder fears about the proverbial permanent record indirectly. FERPA employs what I call a "permission slip" mechanism. It conditions disclosure of PII on parental consent or educator approval, but then delegates more specific decisionmaking about substantive issues to the educational actor—the school, LEA, or SEA. The identity of a data user as an educational actor or approved recipient serves as a proxy for substantive rules regarding appropriate use and repurposing of student information. When FERPA was enacted,

[95] *Id. See, e.g.,* Kansas Fact Sheet, *supra* note 38.
[96] Colorado Interview; Georgia Interview; New York Interview; State IT State Interview.
[97] CLIP Children's Privacy Study, *supra* note 28.
[98] US Department of Education, *Best Practices for Data Destruction*, http://ptac.ed.gov/sites/default/files/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D.pdf.
[99] *Id.*
[100] New York Interview.
[101] *Id. See, e.g.*, Colorado Interview; Georgia Interview; State IT State Interview.

detailed requirements and protocols were not necessary because the practical obscurity of physical records severely limited the potential for unauthorized access or inappropriate repurposing.

The efficacy and sufficiency of this regime rests on a degree of trust unsettled by new information practices, technological capabilities, and introduction of third parties integral to the flow of information within the educational system. Authorization may not be sufficient to quell stakeholder fears about third-party mishandling or misuse of student data in the absence of clear authorization criteria, governance and security protocols, and direct accountability mechanisms.[102]

The current system does not directly account for new ways that student information may be repurposed, the difficulty of monitoring and assuring compliance, and FERPA's lack of direct control or sanction on third parties. Further, FERPA's focus on anonymization fails to account for the sensitivity of non-content information like metadata. It does not address the ways that information stripped of personal identifiers may still be associated with specific individuals. Its purpose-based restrictions have become more complicated in the era of big data, when research involves searching for correlations instead of confirming hypotheses, and information is infinitely repurposable.

Focus on Fixes

The current system lacks the transparency, specificity, and accountability necessary to set stakeholders at ease and provide a better basis for policymaking. In response, legislators, advocates, and industry groups have proposed a variety of guidelines and legislative measures to protect student privacy.[103]

States considered 110 bills explicitly addressing student data in 2014. These measures incorporate a variety of approaches to safeguarding student data.[104] Some provisions merely reiterate the protections currently codified in FERPA, like parents' ability to opt out of directory information. Some seek to increase transparency by providing for public lists of state data inventories. Others call for better data governance by designating rulemaking authority or establishing chief privacy officer positions. Several bills imposed requirements on districts regarding contracting with third parties, including baseline data security mechanisms like frequent audits or encryption.

Others created substantive limitations on the type of information that can be collected or the uses and purposes to which information may be applied. Several states prohibited the collection of biometric information related to religious or political affiliation, sexual behavior, gun ownership,

---

[102] *See, e.g.,* Peter Rugh, *Big Brother is Watching...Our Kids' Test Scores*, ALTERNET, 2013, http://www.alternet.org/education/big-brother-watchingour-kids-test-scores?paging=off&current_page=1#bookmark; Molinar, *supra* note 26.

[103] Natasha Singer, *With Tech Taking Over in Schools, Worries Rise*, NEW YORK TIMES (September 14, 2014), http://www.nytimes.com/2014/09/15/technology/with-tech-taking-over-in-schools-worries-rise.html; Data Quality Campaign, *State Student Data Privacy Legislation*, http://dataqualitycampaign.org/files/State%20Student%20Data%20Privacy%20Legislation%20Resource.pdf [hereinafter "DQC State Legislation Summary"].

[104] *Id.*

health, and psychological data. Some prohibited specific uses for student information like predictive analytics or advertising.

Senators Edward J. Markey (D-MA) and Orrin Hatch (R-UT) proposed amendments to FERPA in July. The bill, called the Protecting Student Privacy Act, requires schools, LEAs, and SEAs to ensure that outsides parties have adequate data security mechanisms in place to protect FERPA-covered information and extend FERPA rights of access and recordkeeping regarding the request or disclosure of FERPA-protected information.[105] They will also lose federal funding if they knowingly provide access to FERPA-protected information to advertise or market a product or service. The bill, however, still rests on FERPA's permission slip mechanism.

Other measures impose regulatory regimes that apply more directly to third parties and permanent record fears. Of particular note, California recently passed a bill that prohibits online operators from compiling profiles on K–12 students for purposes other than those for which the information was originally collected and data destruction upon students' request.[106] It represents a dramatic shift in regulatory mechanisms that addresses stakeholder fears about the proverbial permanent record more directly by imposing use limitations, data destruction requirements, and liability on third parties.[107]

Recommendations

These measures show that policymakers want to address stakeholder fears, but may not reflect careful consideration of current practices. Stakeholders must be able to depend on an infrastructure of privacy. Schools, districts, state agencies, and third parties, must go beyond FERPA's baseline requirements. The system must provide more transparency, specific standards, and accountability mechanisms to ensure that reforms address stakeholders' concerns.

Inventory

Schools, LEAs, and SEAs need to keep better records of the information flows and the governing policies in place. This information is currently scattered throughout various privacy policies, data handbooks, and separate websites for lower and higher education entities and longitudinal database systems.[108] This inventory should describe the types of PII education and workforce data collected and the purposes for its collection. Each entity should have a data map that enables policymakers and technical staff to understand information flow within the system. This includes examining third parties' collection, storage, and sharing practices. Even if these materials are too complex for a

[105] The Protecting Student Privacy Act," S. 2690, http://www.markey.senate.gov/imo/media/doc/2014-07-14_StudentPriv_BillText.pdf.
[106] The Student Online Personal Information Act, CA LEGIS 839 (2014), 2014 Cal. Legis. Serv. Ch. 839 (S.B. 1177) (WEST).
[107] The bill does not apply to the SEA, but governs information disclosed under the school official exception by schools and districts.
[108] In response to recent inquiries by journalists, several states could not provide precise or concise details about their data collections or provide links to places where the information is publicly available. *See* Abendschein, *supra* note 36.

layperson to understand, they will at least provide easily accessible information for designated decisionmakers.

Transparency

Most schools and districts have not been transparent about their information practices and security measures. Without such disclosure, stakeholders have little information to counter myths about educational information practices and no concrete reason to trust educational intuitions and agencies. Schools, LEAs, and SEAs should provide the public with as much information about these contracts as possible. They should create clear, centralized resources where stakeholders can see detailed information about what data are collected; who can access them; what information is passed along to districts, states, and the federal government; and whether this information is personally identifiable, associated with a unique student identifier, de-identified, or aggregated. States should be sure to specify the purpose or legal requirements that drive the collection of student information, the privacy protections in place, and information retention and destruction policies. An accurate sense of the practices and protections also provides the basis for informed policy decisions.

ED recently released guidance for schools and districts about the transparency required under federal law and optimal practices.[109] Several states have begun to highlight their information practices and privacy and security policies.[110] Others have specific, plain language security and privacy policies addressing typical stakeholder concerns.[111] Some have also begun to disclose more centralized information in response to stakeholder queries by highlighting and summarizing their information practices and privacy and security policies.[112]

Infrastructure

SEAs and the entities they permit to access student information should put formal technological, physical, and personnel protocols into place and update these on a regular basis. Data governance establishes specific procedures, roles, responsibilities, and policies regarding information practices.[113] Good governance practices include documentation and auditing, as well as establishing clear responsibility for specified information, often using data stewards or governance bodies. This should include delineating approval criteria for data sharing requests and authorization. It is especially important that parents, educators, and administrators have a designated place to turn for answers. For data governance and transparency to be effective, stakeholders and educational actors need to know where to turn for answers.

---

[109] US Department of Education, *Transparency Best Practices*, http://ptac.ed.gov/document/Transparency-Guidance.
[110] Colorado, Idaho, and Missouri, for example, have easily readable lists of data elements and corresponding legal requirements.
[111] *See, e.g.,* Michigan SLDS FAQ, *supra* note 28; Alaska SLDS FAQ, *supra* note 34.
[112] Massachusetts Department of Elementary and Secondary Education, *Policies Relating to the Collection and Use of Student Data*, http://www.doe.mass.edu/infoservices/data/DESEstudentData.pdf.
[113] Traveling Through Time 3, *supra* note 62, at 9.

Accountability

The above principles should be incorporated into and tied to accountability measures in all contracts governing the flow of student information between educational actors, including third parties. Contracts should be explicit about the information at issue, purpose for sharing information, services the data will support, protection mechanisms in place, and repurposing and retention limitations. They must specify the purposes served by disclosing student PII and reiterate FERPA's limitation on redisclosing or repurposing this information. Contracts also need to ensure compliance, including audits of third-party security risk assessments, and direct accountability if third parties fail to meet these requirements.

Conclusion

While the protections in place today limit actors' abilities to create a proverbial permanent record, the trend toward more portable, interoperable, durable, and repurposable data must proceed with proper standards in place to guard against systems that might shackle students to their pasts. It is crucial that educators and policymakers improve the privacy infrastructure to determine appropriate data governance, security, and flow of student information. Stakeholders and policymakers must develop standards to make the current regulatory framework better suited to address public concerns.

Industry and advocate guidelines, state action, and ED guidance are a start, but baseline technological, procedural, auditing, and governance protocols must be put into place at the school, district, and state level. Schools and policymakers need to consider the substantive propriety of various information practices and create rules so that there are consequences for actors who intentionally, recklessly, or negligently disclose information to unauthorized parties or repurpose it.

It is also critical to recognize that much of the rhetoric about student privacy conflates information practices with pedagogical, institutional, and educational policy issues. Accordingly, educational actors and third-party providers must be as transparent as possible about the information they collect, how it is stored, who can access it, and what follows a student over the course of his progress through the educational system. In the absence of such transparency, parents may opt out of these systems altogether, creating administrative havoc and increasing the likelihood of skewed datasets.

The conversation needs to focus on actual and proposed practices regarding student information so that schools, policymakers, data stewards, and data governance bodies can determine what protective mechanisms will best address community concerns about the proverbial permanent record while allowing educators and schools to be as effective they can be.