MINING FOR SUCCESS: HAVE STUDENT DATA PRIVACY AND EDUCATIONAL DATA MINING CREATED A LEGISLATIVE WAR ZONE?

Meriem El-Khattabi[*]

TABLE OF CONTENTS

I. INTRODUCTION

Computer literacy is rapidly changing the way students learn on all educational levels. As of 2016, U.S. public schools provided at least one computing device for every five students K-12 and spent over three billion dollars for digital content.[1] Today, throughout the United States, students are entering their usernames and passwords to log into personalized learning websites on their glossy Chromebooks—provided to them by their schools at a steeply discounted price—to take tests, do homework, write e-mails, and even

[*] J.D., University of Illinois College of Law, 2018; M.A., Economics, Boston University, 2015; B.S., Economics and French minor, Emory University, 2014. This note is dedicated to my parents and brothers for their unconditional love and constant encouragement in everything I choose to pursue. Special thanks to Charles J. Tabb, Samuel Branum, Sahrish Moyeed, and the entire Illinois Journal of Law, Technology & Policy members and staff for helping me edit this Note.

[1] Benjamin Herold, *Technology in Education: An Overview*, EDUC. WK. (Feb. 5, 2016), http://www.edweek.org/ew/issues/technology-in-education/index.html.

just surf the web.[2] What is harder to comprehend, however, is the extent to which these activities yield massive streams of personal student information[3] for the emerging discipline of educational data mining (EDM).[4] EDM, a multidisciplinary field that uses educational data to analyze students and their learning environments, requires collecting massive quantities of information, including personal and non-educational data.[5] EDM-based analysis of student data reveals otherwise hidden relationships and patterns within complex datasets.[6]

Alarmingly, this information is routinely being shared with third-party vendors and commercial providers who manage and design these technology-based learning systems.[7] As such, the use of EDM-generated technology poses a unique threat to student data privacy.[8] Student data collection, an essential component of EDM, is increasingly carried out via third-party vendors providing software packages and cloud-based data storage.[9] In this context, EDM and big data have become buzzwords for controversial programs adopted on all public education levels throughout the United States, following students from “cradle-to-career.”[10] The twin issues of student data privacy and the pervasive, but often hidden, use of EDM have created a legislative no man’s land sparking national debate and, in its wake, a flurry of legislative action. This rapid growth of data mining technology to improve U.S. public education has galvanized supporters

[2] *See e.g.*, *Blended Learning Management Systems*, Dig. Learning All., http://www.digitallearningalliance.org/blended-learning-management-systems/ (last visited Oct. 20, 2017) (providing background information on a blended learning approach that uses technology and online learning platforms for classroom instruction).

[3] *See* Kelly Gallagher et al., *The Educator’s Guide to Student Data Privacy*, ConnectSafely (May 20, 2016), https://www.connectsafely.org/eduprivacy/, (defining student data “*as personally identifiable information, or PII, and is subject to additional restrictions in laws and regulations*”) (emphasis in original).

[4] *JEDM—Journal of Educational Data Mining*, J. Educ. Dating Mining, (last visited Oct. 20, 2017), http://www.educationaldatamining.org/JEDM/index.php/JEDM.

[5] Marcelo Tibau, *Educational Data Mining and Learning Analytics*, Marcelo Tibau (Nov. 21, 2016), https://tibau.org/2016/11/21/educational-data-mining-and-learning-analytics/. *See generally Data, Analytics, & Adaptive Learning*, Pearson, https://www.pearson.com/us/higher-education/why-choose-pearson/thought-leadership/data-analytics-adaptive-learning.html (last visited Oct. 20, 2017) (illustrating how educational companies involved in personalized e-learning, such as Pearson, with 11 million student users world-wide, engage in the active gathering, organizing, analysis and sharing of data produced by its users).

[6] Mimi Recker et al., *Educational Data Mining and Learning Analytics*, Ctr. for Innovative Res. & CyberLearning 1 (2014), http://circl.sri.com/archive/primers/CIRCL-Primer-LearningAnalytics.pdf.

[7] *See Education Datapalooza: Unleashing the Power of Open Data to Help Students, Parents, and Teachers*, U.S. Dept. Educ.: Official Blog (Jan. 2013), https://blog.ed.gov/2013/01/education-datapalooza-unleashing-the-power-of-open-data-to-help-students-parents-and-teachers/ (discussing “a collaboration between the U.S. Department of Education and software developers to help students securely export or download their own education data”); *see also* Janice Gobert, *Op-Ed: Educational Data Mining Can Enhance Science Education*, U.S. News & World Rep. (May 13, 2016, 5:27 PM), https://www.usnews.com/news/articles/2016-05-13/op-ed-educational-data-mining-can-enhance-science-education (discussing how student data is accessed).

[8] *The Network*, StriveTogether, https://www.strivetogether.org/the-network/ (last visited Oct. 20, 2017) [hereinafter StriveTogether].

[9] Jennifer Sabourin et al., *Student Privacy and Educational Data Mining: Perspectives from Industry*, 8 Proc. Int’l Conf. Educ. Data Mining 164 (June 2015), http://www.educationaldatamining.org/EDM2015/proceedings/ full164-170.pdf.

[10] StriveTogether, *supra* note 8.

and detractors into opposing groups, locked in a virtual power struggle to determine the legal parameters of privacy rights.[11]

This Note will examine the current trends in EDM-generated learning, also known as predictive analysis,[12] which has created a potential legislative powder keg. Part II will first explore the definition of EDM predictive analysis, focusing on its aims and goals. Special focus will be given to the potential benefits and threats of data mining, identifying the major sector of society this affects. It will then examine the current trends aimed to protect student privacy, looking at self-regulation and the role of advocacy groups.

Part III will analyze the current impetus to introduce state legislation to create a check on the uses and misuses of knowledge gained through EDM. Particularly, it will examine student data privacy, cloud-based EDM technology, and the role of third-party vendors. It will further analyze the merits of introducing stronger bills to protect student and parental privacy rights. Part IV will recommend the need for increased safeguards for both student and parental data privacy within the context of the recent rapid proliferation of EDM.[13] These recommendations will evaluate the pros and cons of EDM and big data collection,[14] keeping in mind the need to protect student and parent privacy rights in an environment that should foster innovation, transparency, and trust.[15]

II. BACKGROUND

A. Educational Data Mining Redefined

While big data in educational settings is still in its early stages, there has recently been a surge, not only in the extent of computational power, but in the real-world application of data-driven technology to shape how students learn in and out of the classroom.[16] Indeed, by 2016, approximately fifty-four percent of K-12 students and teachers had a school-issued personal computing device.[17]

[11] *See Top 12 Concerns About Every Student Succeeds Act (S 1177 & HR 5)*, TRUTH IN AM. EDUC. (Dec. 2, 2015), http://truthinamericaneducation.com/elementary-and-secondary-education-act/top-12-concerns-about-every-student-succeeds-act-s-1177-hr-5/ (outlining main legal concerns with the ESSA and data mining in U.S. public education).

[12] Ryan S.J.d. Baker, *Data Mining for Education*, INTERNATIONAL ENCYCLOPEDIA OF EDUCATION (McGaw, B., et al., eds., 3d ed. 2010) (unpublished manuscript) http://www.columbia.edu/~rsb2162/Encyclopedia%20Chapter%20Draft%20v10%20-fw.pdf.

[13] Brijesh Kumar Baradwaj & Saurabh Pal, *Mining Educational Data to Analyze Students' Performance*, 2 INT'L J. ADVANCED COMPUTER SCI. & APPLICATIONS 63 (2011), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.622.7129&rep=rep1&type=pdf.

[14] Marie Bienkowski et al., *Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics: An Issue Brief*, U.S. DEP'T OF EDUC. 1, 3 (Oct. 2012), https://tech.ed.gov/wp-content/uploads/2014/03/edm-la-brief.pdf.

[15] Joseph M. Miller & Patrick X. Fowler, *It Takes More Than a Village: Protecting Student Privacy in the Age of Big Data*, SNELL & WILMER: CYBERSECURITY & DATA PRIVACY L. BLOG (Feb. 12, 2015), http://www.swlaw.com/blog/data-security/2015/02/12/it-takes-more-than-a-village-protecting-student-privacy-in-the-age-of-big-data/.

[16] Tibau, *supra* note 5.

[17] Michele Molnar, *Half of K-12 Students to Have Access to 1-to-1 Computing by 2015-16*, EDWEEK MKT. BRIEF (Feb. 24, 2015), https://marketbrief.edweek.org/marketplace-k-12/half_of_k-12_students_to_have_access_to_1-to-1_computing_by_2015-16_1/; *see also* Anick Jesdanun, *How Google Chromebooks Conquered Schools*, SCI. X NETWORK (Feb. 10, 2017), https://phys.org/news/2017-02-google-chromebooks-

No longer confined to the arcane domains of academia and educational policymakers, EDM is a burgeoning multi-billion dollar educational technology (ed-tech) industry.[18] The rapid proliferation of EDM in recent years can be attributed to a combination of factors that include an increase in virtual web-based schools and online e-learning systems.[19] Information, gleaned from these personalized online learning systems, is being used to supplement data from more traditional sources, such as student transcripts and behavioral records.[20] Also spearheading EDM's growth are educational stakeholders—namely local educational institutions and state policy makers.[21] It is important to keep in mind, however, that while education reform in the United States falls to the state and local level,[22] the federal government, through the U.S. Department of Education, carries out reform initiatives according to perceived national needs.[23] Beginning in 2009, under the Obama Administration, federal funding projects to states—to establish measurable rubrics for nationwide standards, assessments, and accountability in conjunction with state educators[24]—explicitly track students from K-12 through college and career.[25] Thus, federal educational reform initiatives overlap with state education policy, spurring the use of EDM technology.[26]

As currently defined by the U.S. Department of Education,[27] EDM's focus is to develop new tools for the collection and discovery of data patterns for

conquered-schools.html#jCp (stating that in 2016, Chromebook, powered by Google's operating system, took forty-nine percent K-12 U.S. education market, up from forty percent in 2015 and nine percent in 2013).

[18] *EdTech and Learning Analytics: How are the Data Sharing Technologies Revolutionizing Education?*, GREPSR (June 26, 2014), https://www.grepsr.com/edtech-and-learning-analytics-educational-data/.

[19] *See Meet Our Partners*, COURSERA, https://www.coursera.org/about/partners (last visited Oct. 20, 2017) (stating ed-tech giant Coursera, a technology company based in Mountain View, CA, founded in 2012, is a prime example of a venture-backed online e-learning company. As of February 2017, Coursera had twenty-four million registered users world-wide).

[20] *What is Educational Data Mining (EDM)?*, EDTECHREVIEW (June 22, 2013), http://edtechreview.in/dictionary/394-what-is-educational-data-mining.

[21] *See* BARBARA DEYOUNG, JENZABAR, START SMALL WITH BIG DATA: IMPACTFUL ANALYTICS FOR HIGHER EDUCATION 1 (2015), www.jenzabar.com/wp-content/uploads/2015/11/Jenzabar_BigData_WhitePaper.pdf (last visited Oct. 20, 2017). (stating that higher educational institutions have more access to student data than ever before).

[22] Margaret L. Hadderman, *State vs. Local Control of Schools*, 24 ERIC DIGEST SERIES, https://www.ericdigests.org/pre-927/state.htm (last visited Oct. 20, 2017).

[23] *See generally An Overview of the U.S. Department of Education*, U.S. DEP'T. OF EDUC. (Sept. 2010), https://www2.ed.gov/about/overview/focus/what_pg3.html (providing a general overview of the U.S. Department of Education's responsibilities).

[24] *See Standards, Assessment & Accountability*, U.S. DEP'T. OF EDUC., https://www2.ed.gov/admins/lead/account/saa.html (last visited Oct. 20, 2017) (explaining how student achievement is monitored and how schools are held accountable); *see also Standards, Assessments and Accountability*, CCSSO, http://www.ccsso.org/What_We_Do/Standards_Assessment_and_Accountability.html (last visited Oct. 20, 2017) (providing background information on the Standards, Assessment, and Accountability programs).

[25] *See Curriculum: National and State Standards*, EDUC. WORLD, http://www.educationworld.com/standards/ (last visited Oct. 19, 2017) (listing various national educational standards for major subject areas).

[26] Furthermore, the Race to the Top Assessment Program, authorized under the American Recovery and Reinvestment Act of 2009 (ARRA), provided funding to States to develop data-driven educational programs. *Race to the Top Assessment Program*, U.S. DEP'T OF EDUC. (Aug. 12, 2014), https://www2.ed.gov/programs/racetothetop-assessment/index.html.

[27] Erwin Gianchandani, *Dept. of Education Releases Learning Analytics Issue Brief*, CCC BLOG (Apr. 10, 2012), http://www.cccblog.org/2012/04/10/dept-of-education-releases-learning-analytics-issue-brief/.

educational purposes.[28] In this context, policymakers and EDM supporters alike label student data collection as "scientific inquiry" designed to better comprehend students and their educational environment.[29] To this end, large-scale data must be collected from students enrolled in K-12 institutions in state school districts to develop personalized educational technology.[30] In Chicago, for instance, EDM tools are used to assess student performance in key areas, such as kindergarten readiness, student engagement in enrichment programs, as well as employment success rates.[31] Playing a key role in educational reform and public school planning, EDM-generated tools are, therefore, inextricably linked to its actual application on local, state, and federal levels.[32]

Currently, administrators and educators throughout the United States are using EDM to reevaluate and redesign educational practices and policies.[33] These policies cover budgets, curricula, course planning, and tutoring programs, spanning from EDM to evaluations of student future success.[34] In Illinois, for example, the State Board of Education designates learning standards for all schools in the state based on National State Board Association (NSBA) and federal guidelines.[35] Each individual district, however, is free to develop its own curricula as long as it adheres to these standards and best current practice research.[36] The Wilmette Illinois Public School District 39, for example, adapts its curricula to a technology-driven pedagogy based on personalized differentiated instruction and continually analyzes student data to assess student progress and learning goals.[37] Through EDM predictive analysis, educational institutions' goal is to provide personalized educational services for all K-12 and post-secondary public school system students.[38]

[28] Baradwaj & Pal, *supra* note 13, at 65.

[29] Baker, *supra* note 12.

[30] *See* Bethany Jaeger, *Data Mining*, ILL. ISSUES (June 2009), http://illinoisissues.uis.edu/archives/2009/06/datamining.html (describing how using data sets to track Illinois students will give a comprehensive view of students' educational progress).

[31] *Id.*

[32] THRIVE CHICAGO, http://www.thrivechi.org/ (last visited Oct. 20, 2017).

[33] Joseph Rollinson & Emma Brunskill, *From Predictive Models to Instructional Policies*, 8 PROC. INT'L CONF. EDUC. DATA MINING 179 (June 2015), http://www.educationaldatamining.org/EDM2015/proceedings/edm2015_proceedings.pdf.

[34] Carrie Wells, *Maryland Universities to Use Data to Predict Student Success—or Failure*, BALT. SUN (June 11, 2016, 1:32 PM), http://www.baltimoresun.com/news/maryland/education/bs-md-college-analytics-20160611-story.html.

[35] *See Background on the Common Core State Standards*, NAT'L SCH. BD. ASS'N, https://www.nsba.org/advocacy/federal-legislative-priorities/academic-standards/background-common-core-state-standards (last visited Oct. 20, 2017); *New Illinois Learning Standards Incorporating Common the Core*, SCH. DIST. U46, http://www.edline.net/pages/SDU46/Departments_Programs/Assessment_and_Accountability/New_Illinois_Learning_Standard (last visited Oct. 20, 2017).

[36] *See Wilmette Public Schools: Curriculum & Instruction*, WILMETTE PUB. SCH. DIST. 39, http://www.wilmette39.org/for_students/curriculum___instruction (last visited Oct. 20, 2017).

[37] *Id.*; *see also* Joshua Bleiberg & Darrell M. West, *Using Standards to Make Big Data Analytics that Work*, BROOKINGS (Mar. 7, 2014), https://www.brookings.edu/blog/techtank/2014/03/07/using-standards-to-make-big-data-analytics-that-work/.

[38] Bleiberg & West, *supra* note 37.

B. The Benefits of Educational Data Mining and Predictive Analysis

EDM promises to transform education and revamp the U.S. public school system to deliver more individualized and personalized services.[39] As such, EDM-based educational reform is considered to offer state-of-the-art resources to boost greater learning that will lead to higher retention and graduation rates.[40] Increasingly, EDM is being incorporated into fully integrated software programs and platforms, such as the Google Cloud G-Suite,[41] allowing administrators and educators to acquire and evaluate hidden knowledge contained in educational records. With this knowledge, advisors can quickly identify students at risk to tailor student course selections to better match academic ability, design online lesson plans, tutoring programs, and assess career path choices.[42] Educators, particularly on the college and university levels, advocate this use of EDM data collection, holding that the end justifies the means.[43]

As mentioned above, educators are particularly optimistic regarding current practical applications of EDM to identify students at risk, specifically minority and low-income group students.[44] EDM promises to identify academic "choke points" hindering student success. Since student attrition rates and poor student performance adversely affect academic institutions' reputations, it is not surprising that educators find EDM technology attractive.[45] College leaders, for instance, view EDM-generated technology as the major pathway to meet the U.S. government's 2025 goal to produce 350,000 more career-ready college graduates.[46] More specifically, in Illinois, former State Board of Education Superintendent Christopher Koch initiated the Illinois Longitudinal Data System (ILDS) to track the same group of students in the state's 877 school districts each year from K-12, college, and entry into the workforce.[47] Significantly, participation in the ILDS fulfilled a major requirement for the State of Illinois to receive two federal stimulus grants for the Chicago Public School System.[48] Nationwide educational reform initiatives promoting EDM technology, such as

[39] Tibau, *supra* note 5.

[40] *See* D. Frank Smith, *White House Summit: Analytics Key to Success in Higher Ed*, EDTECH (Dec. 12, 2014), http://www.edtechmagazine.com/higher/article/2014/12/white-house-summit-analytics-key-success-higher-ed (explaining how data systems that track student progress could put dwindling college graduation rates back on track).

[41] *G Suite for Education (Online) Agreement*, GOOGLE FOR EDUC., https://gsuite.google.com/terms/education_terms.html (last visited Oct. 20, 2017).

[42] Wells, *supra* note 34*; see also Technology is Transforming What Happens When a Child Goes to School*, ECONOMIST (July 22, 2017), https://www.economist.com/news/briefing/21725285-reformers-are-using-new-software-personalise-learning-technology-transforming-what-happens (stating that reformers are using new software to personalize learning).

[43] *Technology is Transforming What Happens When a Child Goes to School*, *supra* note 42.

[44] Wells, *supra* note 34.

[45] Ghada Badr et al., *Abstract to Predicting Students' Performance in University Courses: A Case Study and Tool in KSU Mathematics Department*, 82 PROCEDIA COMP. SCI. 80 (Mar. 30, 2016), http://www.sciencedirect.com/science/article/pii/S1877050916300266.

[46] Press Release, The White House, The President and First Lady's Call to Action on College Opportunity (Dec. 4, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/12/04/president-and-first-lady-s-call-action-college-opportunity.

[47] Jaeger, *supra* note 30.

[48] *ISBE Programs: Illinois Longitudinal Data System Project*, ILL. ST. BD. EDUC., https://www.isbe.net/Pages/Illinois-Longitudinal-Data-System-Project.aspx (last visited Oct. 20, 2017).

in Illinois, call for local school boards and individual school officials' full commitment to integrate data analysis into all aspects of primary, secondary, and higher education.[49] From drafting budgets to shaping policies, EDM programs and initiatives promise to open new pathways for local school administrators to boost the quality of education, graduation rates, and shorten time needed to obtain a diploma and better integrate students into the workforce.[50]

C. The Impact of EDM and the Future of Education Technology

Since EDM aims not only to improve the quality of education, but to reduce attrition, boost graduation rates, and promote successful integration into the workforce, educational administrators can observe how big data benefits individual students and society as a whole.[51] The passage of the Every Student Succeeds Act (ESSA) in 2015 represents a watershed in EDM, resulting in what appears to be an irreversible boost to its practical application on all levels of education.[52] ESSA's impact has mobilized K-12 and higher education school administrators throughout the United States to advocate for the collection and evaluation of big data for student and curriculum assessment to follow and guide students from kindergarten through high school graduation.[53] The U.S. Department of Education's 2016 National Education Technology Plan (NETP) is a prime example of educational programs connected to broad policy initiatives spurred by ESSA that relies heavily on EDM technology.[54] As a comprehensive five-year plan, the NETP promises to transform adult education by using technology to increase access to high quality education on local, state, and federal levels.[55] Thus, the marked increase in interactive personalized learning platforms using cloud technology indicates the new direction EDM is taking and ESSA's future influence on the education marketplace.[56] School district administrators are aware of the economic incentive to comply with longitudinal big data collection since compliance can bring the state much needed federal funding for education.[57] On the state legislative level, student privacy acts strive

[49] *See* CU CRADLE2CAREER, http://www.cucradle2career.org/ (last visited Oct. 20, 2017) (implementing the use of EDM predictive analysis educational methodology in public education).

[50] Wells, *supra* note 34.

[51] *Id.*

[52] Every Student Succeeds Act of 2015, Pub. L. No. 114-95, 129 Stat. 1802.

[53] Scott Palmer, *ESSA: Opportunities and Risks*, EDUC. COUNSEL (Dec. 14, 2016), http://educationcounsel.com/essa-opportunities-risks/.

[54] *See Section 4: Measuring for Learning*, OFF. EDUC. TECH., http://tech.ed.gov/netp/assessment (last visited Oct. 20, 2017) (describing the U.S. Department of Education's Technology Plan to gather data and create personalized digital learning experiences).

[55] MICHAEL RUSSELL ET AL., AM. INST. FOR RES., CONNECTED TEACHING AND PERSONALIZED LEARNING: IMPLICATIONS OF THE NATIONAL EDUCATIONAL TECHNOLOGY PLAN (NETP) FOR ADULT EDUCATION 1–2 (May 31, 2013), https://lincs.ed.gov/ publications/pdf/ImplicationsNTEP_AdultEd.pdf.

[56] Nycole Stawinoga, *Passage of ESSA Will Significantly Impact Education Marketplace*, SIIA (Dec. 14, 2015), http://www.siia.net/blog/index/Post/63042/Passage-of-ESSA-Will-Significantly-Impact-Education-Marketplace.

[57] ARIZ. DEP'T. OF EDUC. OFFICE OF DATA GOVERNANCE, STATE-LEVEL STUDENT DATA COLLECTION & PROTECTION 1, 2 (Aug. 2014), https://www.azed.gov/data/files/2014/08/student-data-collection-formatted.pdf.

to address the pressing issue of student privacy through a variety of policies.[58] Such policies include creating district governance structures to develop transparent data policy guidelines and prohibiting specific uses of sensitive student data for all users.[59] In 2013, Oklahoma legislators created the Student Data Accessibility, Transparency and Accountability Act (Student DATA Act),[60] which requires public reporting of student data collected by the state and mandates creation of a statewide student data security plan.[61] This Act limits data that can be collected on individual students and how that data can be shared to federal, state, or local agencies and organizations outside Oklahoma.[62] It also restricts the state from requesting delinquency and criminal records, medical and health records, Social Security numbers, and biometric information from the student data collected by local schools and districts.[63] Oklahoma's 2013 Student DATA Act and California's landmark 2014 Student Online Personal Information Protection Act (SOPIPA) stand as models for state-level legislation regarding student privacy protection.[64] SOPIPA was the first student data privacy act to prohibit online and cloud-based sites, services, and applications from "using, selling, disclosing, and engaging in targeted marketing with K-12 student data."[65] Other state legislatures building upon SOPIPA's landmark template include Alabama and Connecticut.[66]

Significantly, the Illinois Senate Bill 1828, introduced in 2009, specifically instructs the State Board of Education, Illinois Community College Board, and Board of Higher Education to create longitudinal data systems through data warehouses to link student test scores, length of enrollment, and graduation records for assessment.[67] Current EDM cloud-based management tools allow

[58] *See* Sunny Deye, *Student Data Privacy*, NAT'L CONF. ST. LEGISLATORS (Feb. 10, 2017), http://www.ncsl.org/research/education/student-data-privacy.aspx#2 (discussing increased governance over student confidential information access to educational institutions); *see also* Student Data Accessibility, Transparency and Accountability Act of 2013, H.R. 1989, 54th Leg., Reg. Sess. (Okla. 2013) (enacted), https://www.sos.ok.gov/documents/legislation/54th/2013/1R/HB/1989.pdf (exemplifying an example of new state level legislation regarding student data security).

[59] Deye, *supra* note 58.

[60] *See* Student Data Accessibility, Transparency and Accountability Act, *supra* note 58 (an Oklahoma bill designed to provide guidelines for student data).

[61] Deye, *supra* note 58.

[62] *Id.*

[63] *Id.*

[64] Carrie Coppernoll, *Oklahoma Gov. Mary Fallin Signs Student Privacy Bill*, NEWSOK (June 14, 2013, 4:23 PM), http://newsok.com/article/3851642; Michael Whitener, *State Student Privacy Laws: A Game-Changer for Service Providers*, IAPP (Nov. 23, 2015), https://iapp.org/news/a/state-student-privacy-laws-a-game-changer-for-service-providers/.

[65] Katherine P. McGrath, *Developing a First Amendment for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Protection Act*, 49 U.C. DAVIS L. REV. 1149, 1152 (2013), https://lawreview.law.ucdavis.edu/issues/49/3/Note/49-3_McGrath.pdf.

[66] Sarah Breitenbach, *States Race to Protect Student Data*, PEW CHARITABLE TR.: STATELINE BLOG (June 9, 2016), http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/06/09/states-race-to-protect-student-data.

[67] *See* Longitudinal Education Data System Act, H.R. 107, 96th Gen. Assemb., Reg. Sess. (Ill. 2009), http://www.ilga.gov/legislation/billstatus.asp?DocNum=1828&GAID=10&GA=96&DocTypeID=SB&LegID=40427&SessionID=76 (requiring "the State Board of Education, the Illinois Community College Board, and the Board of Higher Education to jointly establish and maintain a longitudinal data system by entering into one or more agreements that link early learning, elementary, and secondary school student unit records with institution of higher learning student unit records).

Illinois school districts, such as District 308, to update and streamline disparate databases using quantitative business decision-making tools through specialized private companies.[68]

D. Legislative Choke Points and Privacy Threats

EDM privacy threats set the scene for a potential legislative combat zone. The Obama Administration's educational reform bill ESSA effectively transferred significant strategic decision-making power over public school systems away from the federal government and back to state and local levels.[69] Thus, the associated drive to improve school performance and accountability to decrease student attrition and increase graduation rates makes EDM a hot button issue.[70]

Parents and legislators agree that the need to vet technology services and uphold student privacy protection is fraught with difficulty because of the massive amounts of data streams containing personal information.[71] Indeed, improper collection and storage caused by human error puts parents, students, as well as state and local educational institutions at risk of security breaches when this data is processed for use in different databases.[72] This massive collection of data, moreover, often includes highly sensitive identifying personal information, such as Social Security numbers, racial identity, family relationships, disciplinary records, in addition to physical and mental health reports.[73] To make matters worse, participants are often not given the opportunity to opt out of providing personal information.[74]

As reported by the Electronic Frontier Foundation (EFF), a nonprofit privacy watchdog, unchecked educational technology companies are spying on students via school-issued computer devices and EDM communication

[68] Leila Meyer, *Illinois School District Implements Data Warehouse for Analytics*, JOURNAL (Feb. 12, 2014), https://thejournal.com/articles/2014/02/12/illinois-school-district-implements-data-warehouse-for-analytics.aspx.

[69] COUNCIL OF CHIEF STATE SCH. OFFICERS, KEY STATE DECISIONS REQUIRED UNDER THE EVERY STUDENT SUCCEEDS ACT (ESSA), http://www.dpi.state.nc.us/docs/americanindianed/advisory/meetings/2016/02/key-decisions.pdf (last visited Oct. 20, 2017).

[70] *See* Jordan Fabian, *Obama Signs Education Reform Bill*, HILL (Dec. 10, 2015, 11:38 AM), http://thehill.com/homenews/administration/262781-obama-signs-education-reform-bill (describing the educational reform replacing "No Child Left Behind" legislation and abandoning government mandated standardized testing to evaluate student and school system performance).

[71] *See* Press Release, Comm. on Educ. and the Workforce, Subcomm. on Early Childhood, Elementary, and Secondary Educ. Discusses Balance Between Educ. Research and Student Privacy (June 28, 2017), https://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=401813 (discussing effectiveness of the current laws governing education research and student privacy protection).

[72] *See Data Collection and Analysis*, THRIVECHICAGO, http://www.thrivechi.org/approach/data-collection-and-analysis (depicting how Thrive Chicago plans to expand the reach of data tools to other organizations) (last visited Oct. 20, 2017).

[73] Natasha Singer, *InBloom Student Data Repository to Close*, N.Y. TIMES: BITS (Apr. 21, 2014, 1:21 PM), http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/?_r=0.

[74] Leo Hohmann, *Education? No, It's About Data-Mining*, WND (May 10, 2014, 5:52 PM), http://www.wnd.com/2014/05/education-no-its-about-data-mining/ (regarding the opt-out movement and the impact of ESSA in default systems).

services.[75] Education technology service providers, such as Google and Edmodo, exploit data streams to provide state-of-the-art adaptive learning platforms.[76] Increasingly, teachers and students are given user-friendly coaching tools and access to communication services such as live chat, e-mail accounts, and third-party educational applications, ostensibly free of charge.[77] While this may appear to be a positive trend in modern education, important questions arise as to the costs and benefits of these free ed-tech products for consumers since, as in the case of Edmodo, hidden tracking systems monitor teachers and students for advertising purposes.[78] In this context, major dangers of EDM include the contractual sale of sensitive personal data to third-party vendors, often purely for financial gain, exposing student accounts to volatile cyber-attacks ranging from targeted advertising to identity theft.[79] The recent April 2017 Edmodo data breach exposed the dark side of EDM technology to student data privacy as hackers stole personal data pertaining to seventy-seven million users on the K-12 level and subsequently offered the data for sale on the black market.[80]

The risk to student privacy rights posed by for-profit communication companies and software developers, such as Edmodo, demonstrates the need for high security measures to protect student data.[81] On the federal level, the 1974 Family Educational Rights and Privacy Act (FERPA) remains the mainstay of

[75] Benjamin Herold, *Privacy Watchdog Raises Alarms About "Spying" on Students Via Ed Tech*, EDUC. WK.: DIGITAL EDUC. (Apr. 18, 2017, 4:28 PM), http://blogs.edweek.org/edweek/DigitalEducation/2017/04/privacy_watchdog_raises_alarms_edtech_spying.html.

[76] *See* Jenny Abamu, *Edmodo's Tracking of Students and Teachers Revives Skepticism Surrounding 'Free' Edtech Tools*, EDSURGE (May 15, 2017), https://www.edsurge.com/news/2017-05-15-edmodo-s-tracking-of-students-and-teachers-revives-skepticism-surrounding-free-edtech-tools (explaining how EdModo had been tracking students and teachers for advertising services); *see also* Natasha Singer, *Data Security Is a Classroom Worry, Too*, N.Y. TIMES (June 22, 2013), http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html?mcubz=0 (explaining how some learning networks do not protect students' personal information with site-wide encryption).

[77] *See* Janet Wagner, *Education Technology Trends—Part III—Adaptive Learning, Legacy Systems Integration*, PROGRAMMABLEWEB (Aug. 26, 2013), https://www.programmableweb.com/news/education-technology-trends-part-iii-adaptive-learning-legacy-systems-integration/2013/08/26 (noting the increase in the availability of adaptive technology learning platforms); Abamu, *supra* note 76.

[78] Bill Fitzgerald, *Tracking of Teachers and Students in Edmodo*, FUNNYMONKEY (May 14, 2017), https://funnymonkey.com/2017/tracking-of-teachers-and-students-in-edmodo; Benjamin Herold, *Google Acknowledges Data Mining Student Users Outside Apps for Education*, EDUC. WK.: DIGITAL EDUC. (Feb. 17, 2016, 2:57 PM), http://blogs.edweek.org/edweek/DigitalEducation/2016/02/google_acknowledges_data_mining_GAFE_users.html.

[79] *See* Dian Schaffhauser, *Where Data Mining, Privacy Policies, and Identity Theft Intersect*, CAMPUS TECH. (Feb. 12, 2010), https://campustechnology.com/articles/2010/02/12/where-data-mining-privacy-policies-and-identity-theft-intersect.aspx (explaining that, as with commercial databases, student data becomes increasingly vulnerable to computer breaches and hacking).

[80] Alberto Casares, *Deep Dive into the Edmodo Data Breach*, MEDIUM: 4IQ (June 5, 2017), https://medium.com/ 4iqdelvedeep/deep-dive-into-the-edmodo-data-breach-f1207c415ffb.

[81] Benjamin Herold, *Popular Ed-Tech Platform Edmodo Hacked, Faulted for Ad-Tracking*, EDUC. WK.: DIGITAL EDUC. (May 16, 2017, 3:42 PM), http://blogs.edweek.org/edweek/DigitalEducation/ 2017/05/ed-tech_platform_edmodo_hacked_ad_tracking.html?intc=main-mpsmvs; *see also* Gennie Gebhart, *Spying on Students: School-Issued Devices and Student Privacy*, ELECTRONIC FRONTIER FOUND. (Apr. 13, 2017), https://www.eff.org/wp/school-issued-devices-and-student-privacy (providing recommendations for better protecting student data from risks); *see also* Audrey Watters, *Pearson and Knewton: Big Data and the Promise of Personalized Learning*, INSIDE HIGHER ED (Nov. 1, 2011), https://www.insidehighered.com/blogs/hack-higher-education/pearson-and-knewton-big-data-and-promise-personalized-learning (describing how big data promises to impact higher education through adaptive learning platforms).

parental and student privacy protection.[82] In practice, however, this Act is outmoded and does not provide sufficient protection, given the rapid innovations of big data technology and particularly the outsourcing of personal educational data.[83] It is imperative for lawmakers to understand the dynamics of recent uses of EDM.[84] Thus, efforts to amend FERPA to include electronic and digital data available for use by service providers, contractors, or other parties fail to address how educational agencies or institutions disclose education records without parental consent.[85] Even with proper safeguards, the multiple stages through which student data flows is highly vulnerable and open to potentially volatile student privacy breaches.[86]

Data collection and its real-world application within the context of educational reform create potentially volatile privacy issues linked to legislative action.[87] This situation is exacerbated by the omnipresent nationwide use of third-party cloud-based services to manage student records and generate personalized course selection.[88] A 2013 nationwide study, carried out by Professor Joel Reidenberg of Fordham University's Center on Information Law and Policy (CLIP), found that ninety-five percent of school districts are using these digital products.[89] Yet, given that the vast majority of these outside vendors have no data security requirements in their contracts with schools, the repercussion of cloud computing on student privacy protection issues remains largely unknown both to the public and policymakers.[90]

E. The EDM Student Privacy Battleground

In the context of EDM student privacy threats, the inBloom controversy of 2013–2014 called national public attention to the dangers of EDM-generated

[82] *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T OF EDUC. (June 6, 2015), https://ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[83] *Id.*

[84] *Learning Analytics*, OFF. EDUC. TECH. (Oct. 2012), http://tech.ed.gov/learning-analytics/.

[85] *See* Student Privacy Protection Act, H.R. 3157, 114th Cong. (2015) (amending the Family Educational Rights and Privacy Act of 1974 (FERPA) to require educational agencies to protect student records and notify parents of any breaches).

[86] Benjamin Herold, *Messer-Polis Data-Privacy Bill Endorsed by Educator Groups; Industry Wary*, EDUC. WK.: DIGITAL EDUC. (Apr. 29, 2015, 12:00 PM), http://blogs.edweek.org/edweek/DigitalEducation/2015/04/messer-polis_data_privacy_bill_reaction.html.

[87] *See* Cory Bennett, *Senators Unveil Student Data Privacy Bill*, HILL (May 13, 2015, 1:50 PM), http://thehill.com/policy/cybersecurity/241941-bipartisan-bill-to-secure-student-data-hits-senate (explaining that while "[d]ata analysis holds promise for increasing student achievement . . . it also holds peril from a privacy perspective").

[88] *See* Julia Freeland Fisher, *Education Innovation in 2017: 4 Personalized Learning Trends to Watch*, CHRISTENSEN INST.: BLOG (Jan. 4, 2017), https://www.christenseninstitute.org/blog/education-innovation-2017/ (describing how throughout 2016 cloud-based learning platforms proliferated beyond their original founding school networks).

[89] Cory Bennett, *Senators Offer Rival Bill on Student Data Privacy*, HILL (July 16, 2015, 1:17 PM), http://thehill.com/policy/cybersecurity/248196-senate-gets-second-student-data-privacy-bill.

[90] *See* Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools*, CTR. ON L. & INFO. POL'Y 1, 2 (Dec. 13, 2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip (describing how school district cloud service agreements do not provide for data security in contrast to FERPA, which does generally require school districts to maintain direct control of student information when disclosed to third-party service providers).

educational programs.[91] InBloom Inc., a nonprofit organization funded through grants from the Gates Foundation and Carnegie Corporation for the Advancement of Teaching, designed a multi-state cloud data storage facility to collect and format student data.[92] This storage facility then made student data available to third-party data mining vendors.[93] The ensuing national debate, fostered by the parent advocacy group Parent Coalition for Student Privacy, focuses on parental rights and privacy concerns over the collection, storage, and control over this student data.[94]

As of 2016, parents of public and charter school students are increasingly incensed over escalated pressure by school boards, and even ed-tech companies, to participate in invasive EDM learning programs.[95] Parents complain that there is no effective line drawn to prevent legitimate services from straying into uncharted territory that trespasses on student data privacy rights.[96] Significantly then, although EDM-generated programs have been available in public schools for over a decade, current stricter federal reporting requirements show thousands of schools now using online teaching platforms from K-12.[97] No longer a trend or a fad, educational institutions throughout the United States are embracing online adaptive learning using EDM-generated software and coaching tools.[98] Instead of turning the pages of textbooks, students are now required to log into their personalized accounts to study lessons, take tests, and do homework, write e-mails, and chat or surf the web on school-issued computers and mobile devices preloaded with software provided for free or at steep discounts.[99]

Student privacy risks exist because cloud-based educational platforms compile big data that not only include student administrative and academic records, but also highly detailed information known as metadata.[100] Metadata collection entails invasive scans of individual personal Internet and e-mail habits

[91] Ben Kamisar, *Lawsuit Filed in New York to Halt inBloom Program*, EDUC. WK.: DIGITAL EDUC. (Nov. 13, 2013, 12:08 PM), http://blogs.edweek.org/edweek/DigitalEducation/2013/11/lawsuit_filed_in_new_york_to_h.html?ga=1.45348707.659755846.1478787447.

[92] Singer, *supra* note 76.

[93] *Id.*

[94] *InBloom Background*, PARENT COAL. FOR STUDENT PRIVACY, http://www.studentprivacymatters.org/background-of-inbloom/ (last visited Oct. 20, 2017).

[95] Tibau, *supra* note 5.

[96] Leonie Haimson, *Parents Rebel Against Summit/Facebook/Chan-Zuckerberg Online Learning Platform*, PARENT COAL. FOR STUDENT PRIVACY (Aug. 31, 2017), https://www.studentprivacymatters.org/parents-rebel-against-summitfacebookchan-zuckerberg-online-learning-platform/.

[97] *See* Jan Hoffman, *I Know What You Did Last Math Class*, N.Y. TIMES (May 4, 2008), http://www.nytimes.com/2008/05/04/fashion/04edline.html ("Pinnacle Internet Viewer and PowerSchool . . . [software] is used by thousands of schools, kindergarten through 12th grade. PowerSchool alone is used by 10,100 schools in 49 states.").

[98] *See generally* Will Oremus, *No More Pencils, No More Books*, SLATE (Oct. 25, 2015, 8:26 PM), http://www.slate.com/articles/technology/technology/2015/10/adaptive_learning_software_is_replacing_textbooks_and_upending_american.html (explaining how artificially intelligent software is changing American education).

[99] Abamu, *supra* note 76.

[100] *See* Benjamin Herold, *Lawsuit Alleges That Google Has Crossed a 'Creepy Line' with Student Data*, HUFFINGTON POST (Mar. 17, 2014, 2:49 PM), http://www.huffingtonpost.com/2014/03/17/google-data-mining-students_n_4980422.html (explaining that even though Google agreed to stop scanning student personal email accounts, it continues to track individuals' school records and regular computer use).

via automated default processes.[101] For this reason, educational services increasingly embed hidden processes that can closely monitor student computer habits. Indeed, these processes are able to track students' eye movements, key stroke patterns, and facial expressions as they write homework, private e-mails, conduct Internet searches, shop online, as well as use integrated educational software programs such as interactive games.[102] Currently, cloud-based learning platforms, such as G-Suite (formerly known as Google Apps for Education (GAFE) and renamed in September 2016),[103] routinely sift through student data applying methods and algorithms designed for business use.[104] In December 2015, the EFF filed a complaint against Google with the Federal Trade Commission to raise awareness about the privacy dangers of school-supplied electronic devices and software.[105] The EFF complaint claims that the Chrome browsers' unchangeable sync default settings, which are integrated in Google's GAFE software, invade student and parental privacy rights.[106] While Google allegedly uses this data solely to improve and develop new educational digital services,[107] this unchangeable sync default gives virtually unfettered access to student Internet searches, saved passwords, and websites viewed by K-12 students on the Google-distributed laptops.[108] Indeed, Google is often criticized because its terms of service and student privacy policy suffer from opaque language and complex service agreements, implying contractual obligations embedded in the fine print of End User License Agreements (EULA).[109]

Most recently, in January 2017, concern over Google's G-Suite student tracking, profile building, and lack of transparency prompted the Mississippi Attorney General's (AG) Office to sue Google.[110] At the heart of the suit is Google's alleged violation of the Mississippi Consumer Protection Act[111] and failure to comply with its 2015 public commitment to abide by the "K-12 School

[101] *Id.*

[102] Kenneth R. Koedinger et al., *Data Mining and Education*, 6 WIREs COGNITIVE SCI. 333 (Apr. 29, 2015) http://wires.wiley.com/WileyCDA/WiresArticle/articles.html?doi=10.1002%2Fwcs.1350.

[103] *About the Name Change from Google Apps to G Suite*, GOOGLE, https://support.google.com/a/answer/7126147?hl=en (last visited Oct. 20, 2017).

[104] *See* Sue Scheff, *Google Apps for Education: Data Mining and the Threat to Student Privacy*, HUFFINGTON POST, http://www.huffingtonpost.com/sue-scheff/google-apps-for-education_b_5083478.html (last updated June 9, 2011) (pointing to EDM platforms that uncover hidden meaning and patterns useful for scientific and business purposes).

[105] Press Release, Nate Cardozo & Sophia Cope, Electronic Frontier Found., Google Deceptively Tracks Students' Internet Browsing, EFF Says in FTC Complaint (Dec. 1, 2015), https://www.eff.org/press/releases/google-deceptively-tracks-students-internet-browsing-eff-says-complaint-federal-trade.

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *See* Annalee Newitz, *Dangerous Terms: A User's Guide to EULAs*, ELECTRONIC FRONTIER FOUND. (Feb. 17, 2005), https://www.eff.org/wp/dangerous-terms-users-guide-eulas (listing deceiving EULA terms that could hurt consumers); *see also* Off. of Info. & Tech. Mgmt., *Admin. Requirements for the Use of Websites, Computer Applications & Online Resources*, SCH. DISTRICT OF PHILA. (last updated Feb. 2016), https://sites.google.com/a/philasd.org/studentdataprivacy/administrative-requirements (providing a list of contractual requirements set forth by Google).

[110] Press Release, Office of the Attorney Gen. State of Miss., AG Hood Files Suit Against Google over Handling of Student Data (Jan. 17, 2017), http://www.ago.state.ms.us/ag-hood-files-suit-against-google-over-handling-of-student-data.

[111] Jeff Amy, *Mississippi Sues Google, Saying It Violates Student Privacy*, AP NEWS (Jan. 17, 2017), https://www.apnews.com/4996845f6d004089af708e258fcdf512.

Service Provider Pledge to Safeguard Student Privacy" (Pledge).[112] Under this Pledge, Google is not allowed to "collect, maintain, use or share student personal information beyond" the scope "needed for authorized educational/school purposes."[113] Furthermore, any information Google does collect must be disclosed "in a manner easy for parents to understand," specifying "what types of student personal information [are] collect[ed], if any, and the purposes for which the information . . . is used or shared with third parties."[114] The AG accuses Google of failing to abide by Google's own privacy policies, terms of service, contracts, and agreements to advance its business interests and increase its revenue.[115] The AG Office's goal is to uncover Google's non-educational data mining activities[116] and determine the extent of Google's marketing of student information to third parties.[117] Seeking a court order for Google to cease these practices and fully disclose its handling of student data,[118] the AG reiterated the necessity for school administrators to research technology services used by students.[119]

School districts using EDM personalized platform systems are not always able to control the complex process of massive data collection and storage.[120] Currently, parental right advocates are concerned about the California-based Summit's Charter Public School's Personalized Learning Platform, Summit Basecamp.[121] This learning platform has been in use since 2011,[122] developed in partnership with social media company Facebook and backed by CEO Mark Zuckerberg's funding since 2013.[123] Hailed as the school system of the future because of its reported success with low-income students, Summit Basecamp's free-of-charge learning platform is rapidly expanding its influence as it is integrated into charter and public school programs throughout the United States, adding 100 new schools to its network during 2016.[124] Significantly, Summit

[112] Linn Foster Freedman, *Mississippi AG Sues Google for Collection of Student Data*, ROBINSON & COLE: DATA PRIVACY & SECURITY INSIDER (Jan. 19, 2017), https://www.dataprivacyandsecurityinsider.com/2017/01/mississippi-ag-sues-google-for-collection-of-student-data/.

[113] *Id.*

[114] *Id.*

[115] Benjamin Herold, *Mississippi Attorney Gen. Sues Google over Student-Data Privacy*, EDUC. WK.: DIGITAL TECH. (Jan. 19, 2017, 5:35 PM), http://blogs.edweek.org/edweek/DigitalEducation/2017/01/mississippi_sues_google_student_data_privacy.html.

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] Press Release, Office of the Attorney Gen. State of Miss., *supra* note 110.

[120] THRIVECHICAGO, *supra* note 72.

[121] Emma Brown & Todd C. Frankel, *Facebook-Backed School Software Shows Promise–and Raises Privacy Concerns*, WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/local/education/facebook-backed-school-software-shows-promise—and-raises-privacy-concerns/2016/10/11/2580f9fe-80c6-11e6-b002-307601806392_story.html?utm_term=.abcdb1490beb.

[122] *About Summit Public Schools*, SUMMIT LEARNING, https://www.summitlearning.org/about-us (last visited Oct. 20, 2017).

[123] Emma Brown & Todd C. Frankel, *Education Tool Tests Parents' Privacy Fears*, STANDARD-EXAMINER (Oct. 11, 2016, 6:00 PM), http://www.standard.net/National/2016/10/11/Education-tool-tests-parents-privacy-fears.

[124] Benjamin Herold, *Summit Public Schools Expands Personalized Learning Network*, EDUC. WK.: DIGITAL TECH. (Aug. 9, 2016, 5:12 PM), http://blogs.edweek.org/edweek/DigitalEducation/2016/08/summit_public_schools_expands_basecamp.html.

requires parents to sign a consent form, allowing student data to be shared without express consent.[125] This blanket consent form allows third parties to share data, including names, e-mail addresses, schoolwork, grades, and Internet activity.[126]

Parents in favor of Summit Basecamp, however, interpret Summit's privacy policy and terms of service as a robust promise to safeguard the use of student information.[127] Summit is a volunteer signatory of the national Student Privacy Pledge (SPP).[128] The SPP, created by the Future of Privacy Forum and the Software and Information Industry Association, aims to build trust regarding student privacy protection.[129] Signing the SPP signifies that the school service provider agrees to handle the collection, maintenance, and use of student personal information in ongoing industry practices that meet and exceed all federal requirements.[130] Significantly, the SPP applies to all student personal information, even if it is not part of an "educational record" as defined by federal law.[131] Yet, per the SPP website, it is "not intended as a comprehensive privacy policy nor to be inclusive of all requirements to achieve compliance with all applicable federal or state laws."[132]

In this vein, Summit strives to gain trust by using clear, straightforward language indicating that "the Summit Learning Platform contains no advertising and does not use student data for advertising of any kind. Summit does not and will not sell student personal information."[133] According to Summit, although student data is and can be shared with third parties, the use of student information is strictly limited to authorized educational purposes and not used for targeted advertising.[134] Yet, Summit ultimately must rely on these third parties, which may not be committed to adhere to best industry practices "to employ reasonable and comprehensive data protection and security protocols to protect student data."[135] Targeted ads and other related unauthorized use of student data undermines parental and student privacy as it often uses stealthy big

[125] Leonie Haimson, *Serious Privacy Concerns with the New Summit/Facebook Platform, Used in 100 Schools Across the Nation*, N.Y.C. PUB. SCH. PARENTS (Oct. 12, 2016), http://nycpublicschoolparents.blogspot.com/2016/10/serious-privacy-concerns-with-new.html.

[126] *Id.*

[127] Emma Brown & Todd C. Frankel, *Facebook-Backed School Software Shows Promise—and Raises Privacy Concerns*, WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/local/education/facebook-backed-school-software-shows-promise—and-raises-privacy-concerns/2016/10/11/2580f9fe-80c6-11e6-b002-307601806392_story.html?utm_term=.264cff16423c.

[128] *See Signatories*, STUDENT PRIVACY PLEDGE, https://studentprivacypledge.org/signatories/ (listing service providers encouraged to clearly articulate privacy protection practices to further ensure confidence in how they handle student data) (last visited Oct. 20, 2017).

[129] *See id.* (restricting collection and distribution of student data regardless of whether a formal contract exists with the school).

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Who Has Access to Student Data? What is the Role of Third Parties?*, SUMMIT LEARNING, https://help.summitlearning.org/hc/en-us/articles/223006188-Who-has-access-to-student-data-What-is-the-role-of-third-parties- (last visited Oct. 20, 2017) [hereinafter SUMMIT LEARNING].

[134] Doug Mesecar, *Protecting Student Privacy and Producing Academic Results with Summit's Learning Personalized Platform*, BLENDED LEARNING FACTS (Oct. 14, 2016), http://www.blendedlearningfacts.com/protecting-student-privacy-and-producing-academic-results-with-summits-personalized-learning-platform.

[135] SUMMIT LEARNING, *supra* note 133.

data tracking methods, particularly through social networking sites, such as Facebook.[136] Furthermore, as it is unclear whether this data qualifies as part of a student's educational records, the trail of student digital data and metadata from personalized adaptive learning platforms may not fall under the purview of FERPA protection.[137] FERPA expressly precludes the disclosure of educational information without the prior approval of the student or parent.[138] To date, however, FERPA does not clearly define "educational information."[139] Accordingly, the fundamental assault on parental and student rights posed by gaps in FERPA regarding EDM and cloud technology educational platforms has pressed the American Civil Liberties Union (ACLU) into action to aid school districts through the creation of standardized model legislation templates.[140] Similarly, the 2014 Electronic Privacy Information Center (EPIC) proposal for a Student Privacy Bill of Rights (SPBR) aims to create enforceable student privacy and data security best practice guidelines based on existing consumer and fair practice frameworks.[141]

In line with the need for federal reform, rival bipartisan congressional bills aiming to update FERPA were introduced during 2014–2015 but subsequently withdrawn. They include the Daines-Blumenthal SAFE KIDS Act (S.1788), the Messer-Polis Student Digital Privacy and Parental Rights Act (H.R. 2092), and the Hatch-Markey Protecting Student Privacy Act of 2015 (S. 1322).[142] These attempts to reform FERPA address the need for stronger regulations to control third-party entities that are granted access to educational records containing personally identifiable and other student data.[143] Yet, while data privacy experts from EPIC's non-profit student privacy project view bills, such as those proposed by Messer-Polis, as a step in the right direction, they propose a template for a Student Data Privacy Bill of Rights (SDBR) that would serve as

[136] Peter Eckersley, *How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them)*, ELECTRONIC FRONTIER FOUND. (Sept. 21, 2009), https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks.

[137] Logan Koepke, *Pending Bills Aim to Define Student Privacy in Digital Age*, EQUALFUTURE (July 22, 2015), https://www.equalfuture.us/2015/07/22/pending-bills-aim-to-define-student-privacy-in-digital-age/.

[138] George C. Hlavac, Esq. & Edward J. Easterly, Esq., *FERPA Primer: The Basics and Beyond*, NAT'L ASS'N OF COLLEGES & EMPLOYERS (Apr. 1, 2015), http://www.naceweb.org/public/ferpa0808.htm.

[139] *See id.* (defining FERPA as "education records," as "records, files, documents, and other materials . . . maintained by an educational agency or institution, or by a person acting for such agency or institution." This definition includes student transcripts, GPA, grades, social security number, and academic evaluations, and certain psychological evaluations from any and all educational institutions attended by the student).

[140] *See Student Information Systems (Student Data Privacy) Model Legislation*, ACLU, https://www.aclu.org/legal-document/student-information-systems-student-data-privacy-model-legislation (detailing legislation proposed by the ACLU) (last visited Oct. 20, 2017); *see also 1-to-1 Programs (Student Data Privacy) Model Legislation*, ACLU, https://www.aclu.org/legal-document/1-1-programs-student-data-privacy-model-legislation (detailing legislation proposed by the ACLU) (last visited Oct. 20, 2017).

[141] *Student Privacy Bill of Rights*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/student/bill-of-rights.html (last visited Oct. 20, 2017).

[142] Cory Bennett, *Senator Eyes Fall For Action on Student Data Privacy Bill*, HILL (July 20, 2015, 5:10 PM), http://thehill.com/policy/cybersecurity/248553-senator-eyes-fall-for-student-data-privacy-bill.

[143] *Legislative Priorities in the 115th Congress*, NAT'L ASS'N OF ELEMENTARY SCH. PRINCIPALS, http://www.naesp.org/legislative-priorities-115th-congress (last visited Oct. 20, 2017).

an overarching pledge to identify the fundamental principles and rights underlying student data privacy.[144]

III. Analysis

At present, legislators, educators, parents, and students are locked in a virtual power struggle over who controls highly personal student data.[145] The rapid development of EDM teaching and tutoring systems presents unknown dangers linked to the collection and analysis of a constant stream of personal, highly detailed big data.[146] Technological advances in the field of EDM and the magnitude of data being collected and stored are creating new and hitherto unknown threats to student and family data privacy.[147] Student privacy rights and protection from commercial exploitation are endangered by reliance on cloud-based EDM services using business models that may be commercial, non-commercial, or a mixture of both.[148]

A. The Struggle for Control over Student Data Parent Advocacy

The inBloom privacy controversy of 2013–2014 brought EDM and student privacy to the forefront of public attention.[149] This controversy centered on a national debate over how data-driven educational reform policy may increase privacy risks because of data outsourcing.[150] Parent advocacy groups resisted the introduction of state-run educational programs handled through inBloom, not just because of a loss of control over the use of student data, but also because of the vulnerability of unprotected cloud storage and servers linked to undisclosed third-party vendors through ambiguous and often covert agreements granting data sharing roles.[151]

[144] *See Student Privacy Bill of Rights*, *supra* note 141 (listing practices cloud-based service providers should adhere to when amassing student data). *See also* Cory Bennett, *Bipartisan Student Data Privacy Bill Hits House*, HILL (Mar. 23, 2015, 9:47 AM), http://thehill.com/policy/cybersecurity/236588-bipartisan-student-data-privacy-bill-hits-house (regarding how the Student Digital Privacy and Parental Rights Act would apply to third-party companies using digital educational services).

[145] *Sensitive Personal Data—Students*, DATA PROT. IN SCH., http://www.dataprotectionschools.ie/en/Data-Protection-Guidelines/Sensitive-Personal-Data/Sensitive-Personal-Data-Students/ (last visited Oct. 20, 2017).

[146] Will Oremus, *No More Pencils, No More Books*, SLATE (Oct. 25, 2015, 8:26 PM), http://www.slate.com/articles/technology/technology/2015/10/adaptive_learning_software_is_replacing_textbooks_and_upending_american.html.

[147] David Bainbridge, *Edtech is the Next FinTech*, TECHCRUNCH (Aug. 13, 2016), https://techcrunch.com/2016/08/13/edtech-is-the-next-fintech/.

[148] Oremus, *supra* note 146.

[149] *InBloom Closes Down*, PURE (Apr. 21, 2014, 3:58 PM), http://pureparents.org/?tag=inbloom.

[150] *Id*.

[151] Daniel R. Stoller, *Student Privacy at Risk Absent Better Training for All*, BLOOMBERG LAW: PRIV.& DATA SEC. (Mar. 28, 2016), http://www.bna.com/student-privacy-risk-n57982069087/; Committee Statements, *Kline Statement: Hearing on "Strengthening Education Research and Privacy Protection to Better Serve Students,"* COMM. ON EDUC. AND THE WORKFORCE (Mar. 22, 2016), http://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=400435.

InBloom's innovative design offers a sophisticated system of third-party vendor contracts, data outsourcing, and unfettered data sharing.[152] Yet, the inBloom controversy is significant because it highlights how the lack of transparency regarding security measures continues to fall between the legislative cracks.[153] Significantly, most outside third-party vendors have no data security requirements in their contracts with schools.[154] For instance, Google uses a gag clause in its negotiations with schools, making it all but impossible for IT professionals to assess the nuances of outsourcing to Google.[155] Therefore, much of what is known about how other schools and universities protect the privacy of their students and faculty cannot be invoked, as it implicitly violates the gag clause.[156] Parent groups, fighting against the invasion of EDM into the public school system, argue that the inability of parents to opt out of such programs and ambiguous, broad privacy terms "basically require parents to give up all rights to their children's privacy."[157] Parent advocacy groups, such as the Parent Coalition for Student Privacy,[158] give this as a compelling reason for parents and students to opt out of the public school system and enter homeschooling.[159]

B. Legislative Action

During 2014–2015, a veritable legislative blitz of state legislative action, largely framed by California's SOPIPA, spurred state policymakers to take defensive action in response to the inBloom controversy as well as the incorporation of national educational programs.[160] During 2014, state student privacy bills focused on data collection at the state level and the federal government's role in collecting and accessing student data.[161] Student data privacy bills limit data use by preventing or prohibiting the certain usage of data, such as for predictive analysis, as well as governing the collection of certain data.[162]

Yet, the 2016–2017 projected expansion of EDM personalized educational platforms, like Summit Basecamp, to U.S. public schools, throughout the nation, is already calling into question the efficacy of SOPIPA and state bills modeled

[152] Leonie Haimson, *FAQ on inBloom Inc., What is the State and your School District Doing?*, N.Y.C. PUBLIC SCH. PARENTS (July 24, 2013), http://nycpublicschoolparents.blogspot.com/2013/07/faq-on-inbloom-inc-what-is-your-school.html.

[153] *See* Sens. Edward J. Markey & Orrin Hatch, *Protecting Student Privacy in the Digital Age*, HILL (May 15, 2015, 6:00 AM), http://thehill.com/opinion/op-ed/241997-protecting-student-privacy-in-the-digital-age (stating that many parents do not know schools are sending their child's data to a private company).

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

[155] *Id*.

[156] *Id*.

[157] Brown & Frankel, *supra* note 123.

[158] *See generally* PARENT COALITION FOR STUDENT PRIVACY, http://www.studentprivacymatters.org/ (last visited Oct. 20, 2017) (referring to Parent Coalition group that protects student privacy).

[159] Brown & Frankel, *supra* note 123.

[160] *Student Data Privacy Legislation: A Summary of 2016 State Legislation*, DATA QUALITY CAMPAIGN (Sept. 26, 2016), https://dataqualitycampaign.org/resource/2016-student-data-privacy-legislation/.

[161] PARENT COALITION FOR STUDENT PRIVACY, *supra* note 158.

[162] *Id.*

on it.[163] While SOPIPA addresses student privacy linked to K-12 school programs through online and cloud-based sites, services, and applications, it largely prohibits these operators from "using, selling, disclosing, and engaging in targeted marketing with K-12 student data."[164] A tandem bill by Assembly member Joan Buchanan, D-Alamo, and approved by the Legislature, addresses this gap in SOPIPA.[165] Buchanan's bill requires student data managed by outside companies to remain the property of school districts and in their control since data-management contracts often award companies full access and use of student records.[166] Understandably, educators and parents alike perceive SOPIPA-modeled state bills as incomplete works in progress in need of constant improvement.[167]

Major criticisms of SOPIPA, and state legislation modeled after it, center on the ambiguity of language used, potential loopholes, and a general lack of transparency.[168] In this context, educators uphold Oklahoma and Alabama's State Board of Education's resolution, passed in 2013, as better templates for state data privacy bills.[169] Oklahoma's Student Data Accessibility, Transparency and Accountability Act (the Act), requires transparent public reporting by the state and mandates of all collected student data.[170] The Act mandates the creation of a statewide student data security plan that includes giving parental notice when student records are destroyed.[171] It further limits personal student data collection restricting the transfer of student data to federal, state, or local agencies and to organizations outside Oklahoma.[172] It also restricts data collection of sensitive personal information, such as Social Security numbers.[173] Similarly, the Alabama bill requires that all individuals with access to student data undergo regular training in data security and data

[163] Dylan Peterson, *Edtech and Student Privacy: California Law as a Model*, 31 BERKELEY TECH. L.J. 961, 963 (2016), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2130&context=btlj.

[164] Katherine P. McGrath, *Developing a First Amendment Framework for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Act*, 49 U.C. DAVIS L. REV. 1149, 1152 (2016), https://lawreview.law.ucdavis.edu/issues/49/3/Note/49-3_McGrath.pdf.

[165] Sharon Noguchi, *California Legislature Passes Stiffest U.S. Bill to Protect K-12 Students' Online Data*, MERCURY NEWS (Aug. 31, 2014, 9:39 AM), http://www.mercurynews.com/2014/08/31/california-legislature-passes-stiffest-u-s-bill-to-protect-k-12-students-online-data/.

[166] *Id.*

[167] Paige Kowalski, *Their Take: Privacy and Education Leaders Debate Parental Consent Requirements*, DATA QUALITY CAMPAIGN (Feb. 25, 2016), http://dataqualitycampaign.org/debating-parental-consent/.

[168] Cooley Alert, *Student Data Privacy: States Keep Up the Momentum*, COOLEY (Oct. 1, 2015), https://ed.cooley.com/2015/10/01/student-data-privacy-states-keep-up-the-momentum/.

[169] *See* Sarah Breitenbach, *States Scramble to Protect Student Data and Privacy*, PBS NEWSHOUR (June 9, 2016, 8:47 AM), http://www.pbs.org/newshour/rundown/states-scramble-to-protect-student-data-and-privacy/ (stating that many states followed Oklahoma's lead in implementing similar data privacy laws for students).

[170] Tanya Roscorla, *Examining the Student Data Privacy Landscape in 2016*, CTR. FOR DIGITAL EDUC. (Oct. 3, 2016), http://www.centerdigitaled.com/k-12/Examining-the-Student-Data-Privacy-Landscape-in-2016.html.

[171] *Id.*

[172] *Id.*

[173] Student Data Accessibility, Transparency and Accountability Act of 2013, 2013 OKLA. SESS. LAW SERV. CH. 356 (H.B. 1989) (West) (codified as amended at OKLA. STAT. tit. 70, § 3–168 (2017)).

privacy laws, as well as oversee district governance and the development of transparent policy guidelines.[174]

Another positive trend is evident in the recently proposed amendment to the Illinois School Student Records Act covering K-12 and higher education.[175] This legislation requires parental consent for the disclosure of personal student data and prohibits the commercialization and sale of protected student data.[176] They do not, however, address the role of cloud-based servers, data sharing, or the legal responsibilities of third-party vendors.[177] Illinois student privacy legislation devolves governance responsibilities to the Illinois Board of Education.[178] Notably, the Illinois act clearly acknowledges the Educational State Board's role to oversee and maintain compliance with FERPA as well as to directly govern data privacy issues.[179]

The need for school board compliance with FERPA reveals that one of FERPA's major shortcomings regarding EDM and student privacy is its inability to prevent disclosure of personal educational records that identify a student by name.[180] Indeed, FERPA only protects student data collected and held directly by an educational institution.[181] FERPA does not protect student information collected or held through outsourced third-party entities not subject to a contract with the educational agency.[182] Legislators agree that this flaw must be overhauled to achieve greater transparency.[183] Specifically, FERPA needs to offer parents the right to access and correct personal data held by private firms and to require that educational institutions make public the list of all outside companies with access to student data.[184] Congressional attempts to close FERPA loopholes highlight the complexity of updating FERPA and the constant need to redefine overly broad terms, such as "student records" and "employment opportunities," within the context of EDM and cloud-based technology.[185] Parent advocacy groups and third-party private companies remain pitted against

[174] Alabama State Board of Education, *To Approve the Alabama State Board of Education Data Governance* Policy, ALABAMA STATE DEP'T OF EDUC. (Oct. 10, 2013), http://www.alsde.edu/sites/boe/_bdc/ALSDEBOE/BOE%20-%20Resolutions_3.aspx?ID=2018.

[175] H.B. 332, 100th Gen. Assemb., 1st Reg. Sess. (Ill. 2017).

[176] *Id.*

[177] *Id.*; *see generally State Student Privacy Laws*, PARENT COALITION FOR STUDENT PRIVACY, http://www.studentprivacymatters.org/state-legislation/ (last visited Oct. 20, 2017) (analyzing different states' student privacy laws).

[178] 105 ILL. COMP. STAT. 10/3 (2017).

[179] 105 ILL. COMP. STAT. 10/3, 10/6 (2017); *see generally* Family Educational Rights and Privacy Act of 1974 (FERPA), Pub.L. 93–380, 88 Stat. 57 (1974) (codified as amended at 20 USCA § 1232g).

[180] Hlavac & Easterly, *supra* note 138.

[181] *Id.*

[182] *Id*.

[183] *Id*.

[184] Cory Bennett, *Senators Unveil Student Data Privacy Bill*, HILL (May 13, 2015, 1:50 PM), http://thehill.com/policy/cybersecurity/241941-bipartisan-bill-to-secure-student-data-hits-senate.

[185] Yizhu Wang, *Congress Seeks to Update Student Data Privacy Law*, EDSCOOP (Mar. 22, 2016, 4:00 PM), http://edscoop.com/congress-seeks-to-update-federal-law-to-protect-student-data-privacy; *see* Caitlin Emma, *Data Privacy Bill in Limbo*, POLITICO (Apr. 2, 2015, 10:00 AM), http://www.politico.com/tipsheets/morning-education/2015/04/data-privacy-bill-in-limbo-feds-test-ways-to-keep-borrowers-in-ibr-high-hopes-for-newtown-inspired-mental-health-bill-212543; *see also* Corry Bennett, *Bipartisan Student Data Privacy Bill Hits House*, HILL (Mar. 23, 2015, 9:47 AM), http://thehill.com/policy/cybersecurity/236588-bipartisan-student-data-privacy-bill-hits-house.

each other over FERPA reform with parents arguing that proposed legislation is too weak and industry representatives arguing it is too strong.[186] On the one side, parent advocacy groups want robust security safeguards and enforcement protections.[187] On the other side, education software developers and service providers fear this extra layer of security will create a maze of conflicting policies, regulations, and contractual obligations hampering their ability to do business.[188] For this reason, private industry firms are pushing for a comprehensive, standardized national reform bill.[189] This bill would preempt state legislation by demarcating a federal legislation ceiling to avoid government overreach.[190]

Strong parental opposition to proposed federal legislation highlights several recurrent themes linking the erosion of student privacy to weak language and ambiguous interpretations of data protection safeguards.[191] For example, the Daines-Blumenthal SafeKids Act requires schools and districts to post contracts and privacy policies to allow personal information to be disclosed to third parties.[192] These provisions primarily target children enrolled in pre-kindergarten and early childhood programs.[193] Yet, in the SafeKids Act, the specific personal student data that could be deleted by parents is not clearly defined, and the notification provisions are unclear regarding how parents could access privacy policies and exercise their rights.[194] Parental objections also focus on the deficiency of security and enforcement provisions.[195] Further criticism centers on parental inability to delete personal data collected by third parties that is not contained in educational records.[196] Furthermore, the SafeKids Act allows contextual and targeted ads based on Internet-activity-generated data mining.[197] For these reasons, the Parent Coalition for Student Privacy hailed its sudden withdrawal for a rewrite in September 2016 as a step forward and an opportunity to elaborate stronger student privacy protection regarding FERPA reform.[198]

[186] *See* Emma, *supra* note 185; *see Blumenthal/Daines Student Privacy Bill; Good Start But Needs Improvement*, PARENT COALITION FOR STUDENT PRIVACY (July 16, 2015), https://www.studentprivacymatters.org/blumenthaldaines-student-privacy-bill-good-start-but-needs-improvement/ (describing parents' dissatisfaction with the student privacy bill); *See Parent Attacked By iNACOL and Her Son's Data Disclosed For Questioning "Blended" Learning*, PARENT COALITION FOR STUD. PRIVACY (Apr. 11, 2016), https://www.studentprivacymatters.org/parent-attacked-by-inacol-and-her-sons-data-disclosed-for-questioning-blended-learning/ (discussing a conflict between a parent and an online education association).

[187] *Five Principles to Protect Student Data Privacy*, PARENT COALITION FOR STUDENT PRIVACY (June 22, 2015), https://www.studentprivacymatters.org/five-principles-to-protect-student-data-privacy/.

[188] Emma, *supra* note 185.

[189] *Id.*

[190] *Id*.

[191] Haimson, *supra* note 152.

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] *Id.*

[196] Hlavac & Easterly, *supra* note 138.

[197] *Parent Coalition for Student Privacy Relieved Daines/Blumenthal Safe Kids Act Pulled*, PARENT COALITION FOR STUDENT PRIVACY (Sept. 20, 2016), https://www.studentprivacymatters.org/parent-coalition-for-student-privacy-opposes-passage-of-dainesblumenthal-safe-kids-act/.

[198] *Id.*

Despite parental pressure to institute strong reform legislation, educators who support the use of EDM technology fear that hastily passed federal and state legislation will unnecessarily constrain the safe use of data as more state schoolboards begin to take on governing roles.[199] This creates confusion, thwarting the need to "adequately balance privacy and data use in education and ensure implementers fully understand policymakers' intent."[200] For instance, a Connecticut privacy bill modeled on SOPIPA, requires local and regional education boards to notify parents electronically every time they sign a new contract with a company.[201] However, according to Amelia Vance, Director of Education Data and Technology for the National Association of State Boards of Education (NASBE) and Policy Counsel at the Future of Privacy Forum (FPF), this notification provision will most likely inundate parents with information.[202] Therefore, this bill will fail to increase transparency of data use or parental rights.[203] Indeed, legislation enacted without due care can produce unintended consequences.[204] For example, requiring schools to destroy student records after a student leaves a school would prevent graduates or transfer students from accessing past transcripts for future use.[205] While state-level legislative action continues to address gaps in student privacy provisions,[206] the relative lull in current state legislative action denotes yet another shift in focus emphasizing the need to proceed carefully when enacting federal-level legislation.[207]

Legislative debates question whether a new national law should focus on responsibility on schools or on vendors with whom schools do business.[208] Despite the recognition that federal-level action is needed to establish regulatory norms for EDM and student privacy, educators and policymakers are currently calling for a moratorium on state and federal legislative action to assess the complexity created by rapid ongoing technological change.[209]

[199] Amelia Vance, *Regulating Student Data Privacy: Don't Throw the Baby out with the Bathwater*, 22 POL'Y UPDATE: NAT'L ASS'N ST. BOARDS EDUC. 1, 1 (Apr. 2015), http://www.nasbe.org/wp-content/uploads/Regulating-Student-Data-Privacy_April-2015.pdf.

[200] Dian Schaffhauser, *Data Privacy Legislation Scrutinized in NASBE Report*, JOURNAL, (Apr. 4, 2016), https://thejournal.com/articles/2016/04/04/data-privacy-legislation-scrutinized-in-nasbe-report.aspx.

[201] Sri Ravipati, *States Include Stricter Language in Student Data Privacy Legislation*, JOURNAL (June 6, 2016), https://thejournal.com/articles/2016/06/01/states-include-stricter-language-in-student-data-privacy-legislation.aspx.

[202] Vance, *supra* note 199.

[203] Kowalski, *supra* note 167.

[204] Cindy Long, *Safeguarding Student Data in a Digital World*, NEA TODAY (June 29, 2016, 11:01 AM), http://neatoday.org/2016/06/29/safeguarding-student-data/.

[205] *Id.*

[206] Leo Doran, *New Model Legislation Addresses Student Data Privacy in 16 States*, CTR. FOR DIGITAL EDUC. (Feb. 10, 2016), http://www.centerdigitaled.com/k-12/New-Model-Legislation-Addresses-Student-Data-Privacy-in-16-States.html.

[207] *Id.*

[208] *Epic Student Privacy Project*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/student/ (last visited Oct. 20, 2017).

[209] Vance, *supra* note 199.

IV. Recommendations

Given the rapid evolution and growth of EDM in education, on federal, state, and local levels, student data protection legislation remains in need of urgent update. The incursion of cloud-based technology and use of third-party vendors calls for legislation with clear, transparent, and unambiguous language. The focus of current and future legislation ought to center on the need to generate standardized, fair data practices not covered by statutes rather than on issues related to the commercialization and marketing of student data.[210]

Privacy protection should strike a balance between student and parental right to control sensitive personal data, while also permitting educational institutions to use "big data" for educational reform. Big data is particularly useful for educational reform because of the vast amounts of minute information that can be collected, collated, and interpreted using complex algorithms within different educational contexts in real time.[211] Personalized assessments, driven by big data, are being used to create customized programs as well as new educational methods for course and curriculum improvements.[212] For this reason, proponents of big data believe that, despite its risks, it is uniquely suited to enhance successful student performance from cradle-to-career, providing optimum personalized education choices and learning for students as they transition from secondary educational institutions and subsequent entry into the job market.[213]

Private cloud-based computer networking used in EDM presents unresolved challenges regarding the shared governance of security, privacy, contractual, and legal responsibilities of the institutions providing and using services.[214] Proponents of cloud-based services argue that because of the opportunistic nature of security attacks, location of servers across multiple jurisdictions is less important than means of access to the data infrastructure.[215] Security risks make school system network servers vulnerable to attack as increasing numbers of interconnected individual users employ multiple devices across different platforms such as laptop computers, tablets, and phones.[216] The chain of responsibility involved in protecting student privacy is further complicated by outsourced third-party platform services that are contracted either as part of comprehensive educational service packages or separately.[217]

[210] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, FORDHAM L. ARCHIVE SCHOLARSHIP & HIST. 877, 879–880 (2002), https://pdfs.semanticscholar.org/cebd/f235a1da7ba7377b3a6e9c17b3021ed143fd.pdf; Breitenbach, *supra* note 66.

[211] Mark van Rijmenam, *Four Ways Big Data Will Revolutionize Education*, DATAFLOQ (Apr. 28, 2016), https://datafloq.com/read/big-data-will-revolutionize-learning/206.

[212] *Id.*

[213] *Id.*

[214] Jaydip Sen, *Security and Privacy Issues in Cloud Computing*, SEMANTIC SCHOLAR 1, 32, https://pdfs.semanticscholar.org/4dc3/70d253020947a8e66b701e12dd0233161229.pdf (last visited Oct. 20, 2017).

[215] *Id.*

[216] Calvin Hennick, *Protecting Your Network from Threats Introduced by Users*, EDTECH (Dec. 20, 2016), http://www.edtechmagazine.com/higher/article/2016/12/protecting-your-network-threats-introduced-users.

[217] *Id.*

Indeed, the End User License Agreement (EULA) for cloud service providers often indemnify the provider from any wrongdoing, thereby shifting all liability, accountability, and responsibility for site usage to the user through the EULA.[218]

As a result, educational institutions and districts have become, de facto, the frontline guardians of their data infrastructures, responsible for adopting security measures to prevent unauthorized access and mitigate malware attacks on their networks.[219] Professor Reidenberg's 2013 CLIP study of student privacy advocates full cooperation between school districts and vendors.[220] On their websites, school districts identify cloud service providers and publicly disclose what kind of student information is being transferred to third parties.[221] To that end, Reidenberg recommends that vendors and districts include explicit contract provisions, detailing how cloud services should be used with student data.[222] To be effective, the role of school boards must, however, be bolstered by additional measures to aid standardized compliance. Best-practice guidelines are of special importance given that recent attempts at congressional FERPA reform, notably the Hatch-Markey, Messer-Polis, and Daines-Blumenthal bills aim to address the gaps created by the impact of new technologies,[223] but ultimately fail to guarantee that "data collected in an educational context can be used only for educational purposes."[224] To this end, companies engaged in EDM activities should be actively involved in establishing the highest best-practice standards by introducing concrete recommendations for privacy and security. An industry-wide pledge to uphold these standards would not only prevent regulatory scrutiny, negative publicity, and civil lawsuits, but it would advance educational innovation and gain consumer trust. Clearly articulated best-practice guidelines must, however, not only dovetail with existing legislation but go beyond it to fill in the legislative gaps created by the rapid development of educational technology.

Privacy protection must extend to all students and levels of education from K-12 through post-secondary institutions. Given the rapid development and pervasive use of cloud-based educational applications accessible through cell phones, computers, and other electronic devices connected to the web, lawmakers should heed parent advocacy groups' call to extend privacy protection to include pre-school and kindergarten.[225] Increasingly, student

[218] 3M, CLOUD COMPUTING IN EDUCATION: REWARDS & RISKS (2015), http://multimedia.3m.com/mws/media/1014393O/cloud-computing-in-education-rewards-risks.pdf.

[219] Doran, *supra* note 206.

[220] Reidenberg et al., *supra* note 90.

[221] *Id.*

[222] Fordham News, *Fordham Law National Study Finds Public School Use of Cloud Computing Services Causes Data Privacy Problems*, FORDHAM NEWS (Dec. 13, 2013), http://news.fordham.edu/inside-fordham-category/fordham-law-national-study-finds-public-school-use-of-cloud-computing-services-causes-data-privacy-problems/.

[223] Benjamin Herold, *Student-Data-Privacy Protections Fall Short, Researchers Contend*, EDUC. WK.: DIGITAL TECH. (Apr. 9, 2015, 12:34 PM), http://blogs.edweek.org/edweek/DigitalEducation/2015/04/student_data_privacy_NEPC_report.html.

[224] Bennett, *supra* note 144.

[225] *See* Todd Engdahl, *Student Data Privacy Bill Gets Unanimous Legislative Approval*, CHALKBEAT (May 5, 2016), http://www.chalkbeat.org/posts/co/2016/05/03/student-data-privacy-bill-gets-unanimous-senate-approval/ (discussing student privacy bill).

Internet profiles are compiled as browser activity is tracked through educational portals used to access educational sites as well as to surf the web, to play games, and to use social media.[226] These rapid technological changes are creating a new educational environment that challenges the narrow, traditional definition of students' formal educational records as limited to graded papers, exams, transcripts, or related filed information.[227] State-level legislation must incorporate the need to create uniform, transparent data-sharing protocols and provide clear steps for parents to opt in or out of third-party vendor services, such as college scholarship searches, that benefit parents and students.[228] Rather than prohibiting or severely limiting data sharing, adoption of provisions such as the legal document templates created by the ACLU[229] would allow parents to direct a vendor to send data selected services as long as transparent, specific permissions and strict protections are provided.[230] For these reasons, educators and parents want the legal burden to protect students' information to include vendors, as well as schools and districts.[231]

Furthermore, school boards and administrators should be held to comply with clear, uniform standards as they take on more responsibility to govern and oversee EDM programs to ensure privacy protection. Indeed, in the wake of ESSA, EDM privacy protection is increasingly a shared venture involving school districts, educational technology companies, and state boards of education.[232] Board participation on state privacy or data commissions should include establishing guidelines for the proper training of staff and volunteers handling personal student digital data. All individuals involved in handling EDM big data should be compelled to undergo standardized specialized training.[233] To carry this out, schools should be required to fully and clearly disclose all contractual partnerships made with third-party vendors such as contractors and consultants, and require parental notification or consent for disclosure of educational records to them. At the same time, schools should also pledge to clearly disclose any use of collected data for the development and sale of educational products across single technological platforms.[234] This pledge would give parents and students an opportunity to opt out if they are not

[226] Alex Molnar & Faith Boninger, *On the Block: Student Data and Privacy in the Digital Age*, NAT'L EDUC. POL'Y CTR. (Apr. 9, 2015), http://nepc.colorado.edu/publication/schoolhouse-commercialism-2014.

[227] *See* Office of the Registrar, *Policies*, IND. UNIV. BLOOMINGTON, http://registrar.indiana.edu/policies/ferpa/student-privacy-introduction.shtml (last visited Oct. 20, 2017) (providing an example of what types of student information is accessible to universities).

[228] *Student Information Systems (Student Data Privacy) Model Legislation*, ACLU, https://www.aclu.org/legal-document/student-information-systems-student-data-privacy-model-legislation (last visited Oct. 20, 2017); Jules Polonetsky & Brenda Leong, *We Must Support Parental Choice for Student Data*, HILL (Sept. 21, 2016, 6:50 AM), http://thehill.com/blogs/pundits-blog/education/296923-we-must-support-parental-choice-for-student-data.

[229] *See 1-to-1 Programs (Student Data Privacy) Model Legislation*, *supra* note 140 (providing an example of a student data privacy legal document template).

[230] Doran, *supra* note 206.

[231] Molnar & Boninger, *supra* note 226.

[232] Stoller, *supra* note 151.

[233] *Id.*

[234] Roscorla, *supra* note 170.

comfortable with the possibility of data being used to generate targeted educational programs, including targeted advertisements.

Moving forward, however, new privacy protection legislation should not focus primarily on marketing or commercialization of educational products. Regulations should address where and for how long data is used and stored. Companies creating EDM educational programs and the institutions implementing them should adhere to a clearly designed set of best-industry-practice policies and pledge to fully disclose data collection use, type of longitudinal study, and source of outside funding. Students and parents should be offered clearly accessible modes to opt out of data sharing as well as to correct or delete data. In this context, the Student Privacy Pledge (SPP) should be strengthened.[235] To be effective, it should establish guidelines for parental and student consent using clearly defined terms that are in harmony with existing legislation. This should be achieved through the avoidance of ambiguous language using an agreed upon lexicon-glossary to define terms such as "personally identifiable information" and "school service" provider. Such a glossary is needed since, if too narrowly interpreted, companies and third-party entities can abuse flaws and loopholes to collect data that ostensibly fall outside the parameters of the SPP as well as FERPA and state legislation.[236]

This creation of an agreed upon glossary of terms would allow legislation on the federal and state levels to adopt a standard for data management, establishing comparable data across all sectors, which is crucial for consistent federal reporting.[237] In particular, state legislation should strive to achieve uniformity, adopting and adapting an unambiguous template, such as California's SOPIPA,[238] with strong enforcement mechanisms and security practices. Clearly defined standardized guidelines should cover the full disclosure of personal data collected by companies and schools, such as home addresses, Social Security numbers, biometric and social media information to bolster transparency and instill confidence, as well as trust, in school administrations invested in digitalized education. Standardized norms should be established for data breach notifications to all institutions and involved individuals.[239] A standardized checklist and schedule should be designed,

[235] *Student Privacy Bill of Rights*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/student/bill-of-rights.html (last visited Oct. 20, 2017).

[236] Gennie Gebhart & Sophia Cope, *Loopholes and Flaws in the Student Privacy Pledge*, ELECTRONIC FRONTIER FOUND. (Oct. 20, 2016), https://www.eff.org/deeplinks/2016/10/loopholes-and-flaws-student-privacy-pledge.

[237] *See* NAT'L CTR. FOR EDUC. STAT., http://nces.ed.gov/ (last visited Oct. 20, 2017) (describing how the Common Education Data Standards initiative (CEDS), which is carried out entirely by volunteers, is working on such an initiative in conjunction with the National Center for Education Statistics (NCES)).

[238] *See generally An Overview of the California Student Data Privacy Agreement*, CAL. STUDENT PRIVACY ALLIANCE, https://secure2.cpsd.us/cspa/agreements/CSDPA_Final_V1_Overview.pdf (last visited Oct. 20, 2017) (describing an overview of SOPIPA).

[239] *See State Student Privacy Policy*, ELEC. PRIVACY INFO. CTR., https://epic.org/state-policy/student-privacy/ (last visited Oct. 20, 2017) (showing that states could build upon SOPIPA's framework by requiring data breach notifications).

instructing educational administrators to regularly review and update data security norms and procedures.[240]

Given the rapid changes in educational technology and its application, state legislation must ensure that data privacy policy measures establish policy guidelines to protect all student data. Because of this shift in EDM, state legislators must build on the SOPIPA template to provide strong state legislation to hold vendors legally accountable for misusing personal student information, including sensitive metadata not considered to be part of official educational records nor covered under SOPIPA or FERPA. State legislation should also implement a revamped data privacy template with provisions modeled after Oklahoma's 2013 Student Act[241] to address clearly defined consumer protection and data breach notification laws. Responsive state legislation should use similar language to facilitate data protection that effectively spans different state jurisdictions. Such a template would help fill the gaps in current legislation, deterring vendors from processing and storing student data in states with differing legal requirements. Such measures should monitor cloud-based platforms because digitalized educational data is stored on servers residing in multiple states, which involve overlapping and often contradictory state jurisdictions. Furthermore, student privacy bills should require that all institutions involved in handling digitalized data agree to transparent disclosure regarding the multiple locations and jurisdictions of data servers, processers, and digital storage facilities. It is also advisable to uniformly regulate terms of service to protect intellectual property rights of parents, students, and teachers from unauthorized use by third-party contracting entities.[242]

To keep pace with rapid, ongoing changes in EDM technology, extra-governmental collaboration and cooperation on state and local community levels must fill any gaps that legislation fails to address.[243] As school systems across the nation adopt cradle-to-career EDM platforms, education departments are asking for help to establish systems of data governance.[244] Data privacy advocacy groups, such as Electronic Privacy Information Center (EPIC), propose a template for a Student Data Privacy Bill of Rights (SDBR).[245] This type of document would serve to further close the legislative gaps that exist on

[240] *See Student Privacy & Data Security Toolkit for School Service* Providers, EDUC. TECH. INDUS. NETWORK OF SIIA, http://www.siia.net/Divisions/ETIN-Education-Technology-Industry-Network/Resources/Student-Privacy-Data-Security-Toolkit-for-School-Service-Providers (last visited Oct. 20, 2017) (explaining how Data Privacy Toolkits are currently available for educators).

[241] *See* Sunny Deve, *It's a Balancing Act When It Comes To Who Should Be Allowed to Use, Manage and Dispose of the Vast Amount of Student Data Piling Up in Cyberspace*, NAT'L CONF. ST. LEGISLATURES (Apr. 1, 2016), http://www.ncsl.org/research/education/student-data-privacy (summarizing Oklahoma's Student Data Accessibility, Transparency and Accountability Act).

[242] *Id.*

[243] Valerie Strauss, *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, WASH. POST (Mar. 6, 2014), https://www.washingtonpost.com/news/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/.

[244] *Data Governance and Student Privacy*, DEP'T OF EDUC. LA. BELIEVES, https://www.louisianabelieves.com/resources/library/data-center/protecting-student-privacy (last visited Oct. 20, 2017).

[245] *Student Privacy Bill of Rights*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/student/bill-of-rights.html (last visited Oct. 20, 2017).

federal, state, and local levels, considering the needs of parents and students.[246] The adoption and adherence to uphold the SDBR would provide clear guidelines that, on the grassroots level, would foster confidence in rapidly evolving student data privacy systems.

V. CONCLUSION

Educational data mining has enormous innovative potential to personalize and improve education, not only by reducing attrition rates, but also by increasing student performance. Yet, as big data threatens to take over U.S. public school system administration, students and parents are targets for surreptitious data collection. The national conversation regarding student privacy must continue to safeguard the use of EDM by encouraging effective congressional legislation and adherence to transparent best-practice policies.

[246] Bradley Shear, *The Student Privacy Bill of Rights*, SHEAR ON SOC. MEDIA L. (Apr. 3, 2014), http://www.shearsocialmedia.com/2014/04/the-student-privacy-bill-of-rights.html.