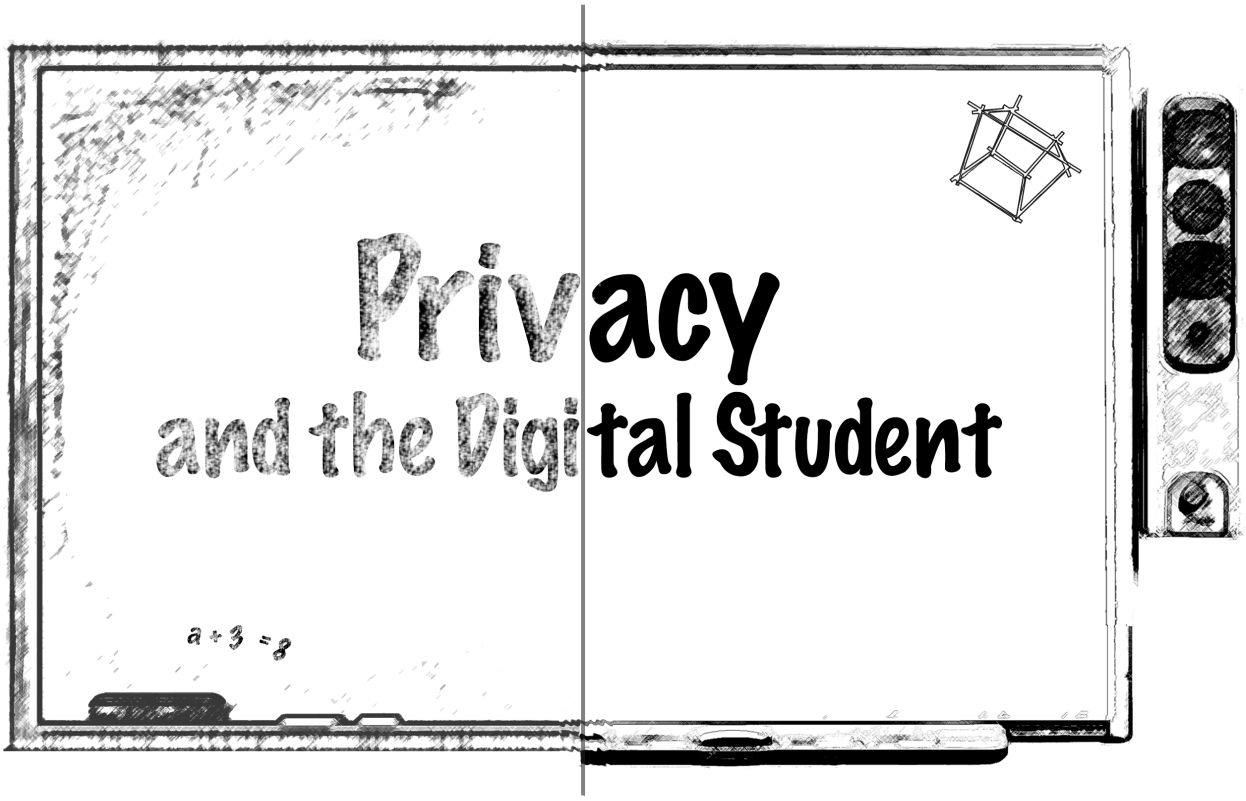
CENTER FOR DEMOCRACY
& TECHNOLOGY

Privacy and the Digital Student



May 2015

PRIVACY AND THE DIGITAL STUDENT

Overview

School districts across the country have embraced education technology ("EdTech") as a means for enhancing school operations and classroom instruction. While the practice of collecting student data is not new – K-12 schools and institutions of higher education have been gathering and reporting test scores, grades, retention records, and the like for years – the means by which student information is collected, the types of information collected, and the entities that ultimately have access to this data have expanded dramatically.[1] We often read news reports on the benefits of technology in the classroom,[2] and EdTech collection practices may prove to revolutionize American education.

At the same time, stories of misuse of student data and poor data security practices in K-12 schools, as well as large-scale breaches of universities' data systems, are increasingly reported.[3] Collection of student data by educational technologies is widespread, though there is not an extensive regulatory framework in place to complement this data collection. Federal student privacy law is outdated and state approaches are inconsistent. Furthermore, federal laws that can be used to reach EdTech directly are limited in their applicability. These gaps in the United States' student privacy legal regime hinders industry innovation and school adoption of EdTech.[4]

CDT believes realizing the full potential of EdTech in the classroom requires robust student privacy standards. Student privacy will be greatly enhanced if the following are accomplished:

The Family Educational Rights and Privacy Act (FERPA) should be amended. For example, the definition of "educational record" likely does not include less traditional data points collected by EdTech, such as meal purchases or geolocation. The definition must be expanded to include such data. Furthermore, the law should provide for broader enforcement penalties (beyond removing all federal funds from a school). This would give the Department of Education more practical means for enforcing the law.

The current federal legislative framework must be updated to encompass EdTech providers. The Children's Online Privacy Protection Act (COPPA) and Federal Trade Commission (FTC) Section 5 authority alone are insufficient to address the role played by EdTech providers in schools. COPPA only applies to online services and websites

---

[1] ISAAC MEISTER & ALICIA SOLOW-NEIDERMAN, K-12 EDTECH CLOUD SERVICE INVENTORY (2014).
[2] Kerry Gallagher, *Balancing Student Privacy with the Benefits of Ed Teach,* THE HILL CONGRESS BLOG (Apr. 27, 2015), http://thehill.com/blogs/congress-blog/education/240026-balancing-student-privacy-with-the-benefits-of-ed-tech.
[3] *See* Natasha Singer, *Data Security is a Classroom Worry, Too*, N.Y. TIMES (Jun. 22, 2013), http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html; *See also* Kyle McCarthy, *5 Colleges with Data Breaches Larger than Sony's in 2014,* HUFFINGTON POST BLOG (Jan. 15, 2015), http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html.
[4] LEAH PLUNKETT ET AL., FRAMING THE LAW & POLICY PICTURE: A SNAPSHOT OF K-12 CLOUD-BASED ED TECH & STUDENT PRIVACY IN 2014 16 (2014).

directed to children under 13 years old, and Section 5 is not written nor designed to address day-to-day privacy best practices; it exists primarily to respond to bad acts. Additionally, it is unclear whether the FTC will use its Section 5 authority to rein in EdTech bad acts with much frequency in the future. Federal legislation should be passed that requires certain privacy-protective measures, broadens the FTC's authority to directly reach EdTech, and explicitly prohibits data collection, use, and sharing practices that go beyond schools' authorizations and students and parents' reasonable expectations.

Data deletion and minimization requirements should be included in legislation, as well as industry and school policies. Companies have the capacity to collect and retain large amounts of highly sensitive data about students, such as tests results, social and emotional assessments, and physical health information. The mere possibility that a data point will be useful in the future should not warrant companies collecting all data and holding on to this data forever. Limits must be placed on collection and retention to offset the potential risk of embarrassing exposure of sensitive information. At the very least, parents and students should be able to request deletion of certain information, and companies should purge data after a certain period, even absent a deletion request.

Sharing limitations should be included in legislation, as well as industry and school policies. The number of entities that have access to student data must be appropriately scoped. Although sharing student data with third parties may be acceptable in certain circumstances – and it would not be practical to obtain user consent for all disclosures to third parties – some sharing arguably would not meet parents and students' reasonable expectation of privacy, and therefore warrants stronger user controls. There should not, for example, be a blanket exception to a law's disclosure limitations and consent requirements for researchers. Some research may have nothing to do with education, and students would not reasonably expect that every element of their performance will be freely shared with any researcher in the name of "Big Data". In such cases, parents and students should have control over whether their data is shared.

This paper explores student data privacy generally. The discussion focuses primarily on student privacy in K-12 schools and includes an overview on both how EdTech is used in schools, and the legal regimes governing this use. It also addresses the above recommendations and reform efforts that have taken place over the past year.

Background

What is "EdTech" and Who Are the Stakeholders?

The term EdTech usually refers to technology used by schools for administration and classroom instruction. Students and parents may also use EdTech outside of school.[5] Stakeholders include school administrators, teachers, parents and students, EdTech suppliers, as well as school district leaders and state and federal departments of education.

[5] Discussed in following sections.

Ways EdTech Collects Student Data

Education technologies collect data both actively (directly soliciting information from users) and passively (collecting data on users that they do not voluntarily share). Collaborative learning platforms, online student record keeping systems, and other services where the company provides a platform encouraging users to share their information are all active data collection. Passive data collection occurs when companies extract data through tracking methods. A common passive data collection technique uses cookies or other unique identifiers to keep track of personal information, such as the frequency of the student's visits to a particular website, the items viewed or services used while on the site, and information the student entered on the specific site.[6] EdTech services can also use other technologies such as JavaScript[7] to trace highly specific information on a student user such as her scrolling pattern on a web page, or time spent answering a question in an online quiz.[8] While both active and passive data collection is expected in certain circumstances, such as when data are used to help the technology function or assist teachers with personalized student instruction, some forms of data collection, like scanning a student's emails to create targeted advertising profiles or selling students' data after a company goes bankrupt, may not meet teachers', parents', and students' reasonable expectations.

How EdTech is Used in Schools

Schools use various technologies on a daily basis, including mobile applications, "connected" ID cards, open source learning modules, and student data repositories. Online cloud computing is one of the most common tools; an estimated 95% of school districts use these services.[9] EdTech serves many functions for schools, including (but not limited to) administrative purposes, classroom instruction, student assessment, Common Core and Statewide Longitudinal Data Systems ("SLDS") implementation, and after-school instruction. Examples include:[10]

> **Administrative purposes.** Schools often use EdTech services to gather and retain student information that would traditionally be collected and maintained by the school, such as student health and attendance records, grades, demographic information or home address and phone numbers.[11] Such practices may be used to increase school efficiency, save storage space on the school's hard drive or in physical files, or simplify the process by which parents can access their students' information. For example, Administrative and Student Information Systems ("SIS") allow teachers and administrators to store, aggregate, and share student

---

[6] Derek S. Witte, *Privacy Deleted: Is It Too Late to Protect Our Privacy Online?*, 17 J. INTERNET L. 1, note 23 at 14 (2014).
[7] *Id.* citing Peter Eckersley, *How Unique Is Your Web Browser?*, PRIVACY ENHANCING TECHNOLOGIES (2010) (Mikhail Atallah, Nicholas Hopper, eds.) ("Using several variables, such as screen resolution, type and version of web browser, system fonts, time zone, plugins, and other settings on a computer, the watchers can run an algorithm that identifies a computer's fingerprint when it is used to visit a Website [without the use of a cookie]").
[8] *Id.*
[9] JOEL R. REINDENBERG ET AL., PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS, Executive Summary (2013).
[10] *See* ISAAC MEISTER & ALICIA SOLOW-NEIDERMAN, K-12 EDTECH CLOUD SERVICE INVENTORY (2014)
[11] *Id.*

information (such as grades, disciplinary or health records) with authorized parties. They are essentially a digital file cabinet containing all student records maintained by the school, as well as information on teacher performance. Pearson Power School, BloomBoard and Illuminate are examples of administrative and SIS platforms. Infrastructure as a Service ("IaaS") provides cloud-based servers and storage for schools. IaaS platforms supplement or altogether replace a school's physical hardware or on-site (school) servers. The servers are located on a third-party site, as opposed to being deployed by the school. Amazon Web Services is an example of this type of platform. Another technology used for school administration is student "smart" ID cards, which are carried by the student throughout the day. They track the student's location and often collect data on the student's entry and exit from school, meal purchases, bus route and attendance through swiping the card's reader at certain checkpoints. ScholarChip is a major provider of student smart cards. [12]

Classroom instruction. Teachers may use EdTech for a range of needs while instructing students. Some services are designed to tailor instruction to a particular student's strengths and weaknesses. Others provide open source learning sites where teachers can access shared lesson plans, videos, handouts, or presentations for use in the classroom. Learning Management Systems ("LMS"), for example, provide teacher-created coursework for students to access online. An LMS may also integrate peer-to-peer grading, social networking, or student-generated content. Edmodo and MyBigCampus are well known LMS. Massive Open Online Courses ("MOOCS"), another form of LMS, provide full courses online. It should be noted that MOOCS are typically used by adults for post-secondary learning, not K-12 students. Coursera, Udacity and edX are popular MOOCS. Collaboration and Identity Platforms bundle services typically used in an office environment (email, documents, Excel, PowerPoint, etc.) into one platform accessible online or on mobile apps. Students submit and share information through these platforms. This information is often supplementary to that contained in a student's file and assists instructors in tailoring their lessons to a student's unique needs. Some platforms seek to create online spaces where users exchange information with one another. Google Apps for Education, a popular collaborative learning system, offers familiar Google services such as Docs, Calendar, Gmail, and search on one central platform managed by the participating school.[13] Office 365 for Education is another example of such a platform.[14]

Student assessment. Data collected on student performance through EdTech is potentially more robust that data collected through traditional assessment methods like paper quizzes and tests. EdTech provides formal and informal student assessment by collecting highly specific data on a student's abilities, such as the

[12] *ScholarChip K-12 Solutions,* SCHOLARCHIP.COM, http://www.scholarchip.com/k12/index.aspx (last visited December 16, 2014).
[13] *Everything Your School Needs,* GOOGLE.COM, http://www.google.com/enterprise/apps/education/ (last visited December 16, 2014).
[14] *See* ISAAC MEISTER & ALICIA SOLOW-NEIDERMAN, K-12 EDTECH CLOUD SERVICE INVENTORY 2 (2014).

time it took for them to answer a particular question, or the pattern of their scrolling habits on a website or app.[15] EdTech can log and categorize numerous data points on a particular student, as well as quickly compare the student to his or her peers or aggregate multiple students' data for an overall picture of a teacher's class. This could create a more comprehensive understanding of student performance throughout the semester or school year. It may also allow school-to-school or state-to-state comparison of student performance – which ultimately informs strategies for future instruction. Standardized testing is almost entirely administered through EdTech today for these reasons. Classroom Feedback Tools assist teachers with student assessment. Platforms like ClassDojo, for example, enable teachers to upload class rosters and document student behavior or accomplishments (such as responsiveness to questions, excitement about particular subject-matter, or misbehaving in class) in real time. Students and parents can then access this feedback from the teacher online, or the teacher can print or email these assessments. Student Data Repositories create a "one stop shop" for teachers and administrators to access students' data. The repository gathers all of the data collected on a student by EdTech and stores it on a central platform. Data repositories may be developed and maintained by school districts to assist with common core or SLDS. InBloom was an example of a student data repository.[16]

After school instruction and studying. Students may complete homework or supplementary study materials at home through EdTech platforms. Some of these services allow teachers to pre-program homework and extra credit assignments. Others provide study aids and materials for students to choose from on their own. Study and Assessment Tools are one type of after-school studying platform that allow students to test their mastery of a subject. These services may provide quizzes, flashcards, or essay prompts for students to access at home. The service grades a student's work or lets teachers grade the student and provide feedback. The platform may also allow for peer review of a student's work product. Quizlet is a popular online study and assessment tool.

It should be noted that this list is not exhaustive. Given the speed by which EdTech is developing, it is possible for schools, students, and parents to use EdTech for a variety of purposes. The opportunities for enhanced learning and school administration through EdTech are great, and therefore the legislative framework accompanying these platforms must be forward-thinking and robust.

[15] Natasha Singer, *Data Security is a Classroom Worry, Too*, N.Y. TIMES (Jun. 22, 2013), http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html.
[16] Ariel Bogle, *What the Failure of inBloom Means for the Student-Data Industry,* SLATE FUTURE TENSE BLOG (Apr. 24, 2014, 3:45 PM), http://www.slate.com/blogs/future_tense/2014/04/24/what_the_failure_of_inbloom_means_for_the_student_data_industry.html.

What Laws Regulate EdTech Data Collection?

Family Educational Rights and Privacy Act ("FERPA")

Under FERPA[17], schools that receive federal funding must not disclose personally identifiable information ("PII") from student educational records to third parties prior to obtaining parental consent. [18] This general rule is subject to exceptions. FERPA allows *directory* PII, such as students' names, addresses, and phone numbers, to be disclosed to third parties without parental consent if the school notifies parents of this practice once a year, and parents are given the opportunity to opt-out of this disclosure.[19] Additionally, the "school officials" exception allows third parties performing school functions or services to collect non-directory PII from a student's educational record without parental consent.[20]

Important terms

- **Educational Records:** Records, files, documents, or other materials that contain information directly related to the student and are maintained by an educational agency or an institution or by a person acting for such agency or institution.[21]
- **Personally Identifiable Information:** Information such as a student's name, address, or phone number, as well as information that alone or in combination with other information is "linkable to a student" or would allow someone to "identify the student with reasonable certainty."[22]
- **Directory Information:** Names, addresses, phone numbers, birth date and place, participation in school activities and sports, and academic record. Directory information may also include a student athlete's height and weight.[23]
- **School Official:** A person or entity that is authorized to receive student PII from an educational record without parental consent. This would include an individual employed by a school or school district who has legitimate educational interests.[24] This may also include a volunteer, contractor, or consultant not employed by the school, provided that the official (1) performs an institutional service or function for which the school would typically use its own employees, (2) has a legitimate educational interest in the educational records, (3) is under the direct control of the school or district with regards to use and maintenance of PII from education records, and (4) uses the educational records only for authorized purposes.[25]

---

[17] 20 U.S.C. §1232g, 30 C.F.R. §99.7 §99.37.
[18] *Id.; See also Basic Concepts and Definitions for Privacy and Confidentiality in student Education Records*, IES SLDS TECHNICAL BRIEF, Nov. 2010, at 1 ("In the context of student education records and FERPA, privacy pertains to the rights of parents and eligible students to inspect and review the students' education records, to seek to amend education records, to consent to the release of personally identifiable information from education records for any disclosures that are not authorized in law, and to refuse to have personally identifiable information that is designated as directory information publicly released").
[19] 20 U.S.C. §1232g, 30 C.F.R. §99.7 §99.37.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] 30 C.F.R. §99.31.
[25] See 34 CFR § 99.31(a)(1)(i).

Why FERPA must be updated

- **It's outdated.** While FERPA was groundbreaking privacy legislation when it was passed in 1974, today the law is inadequate given increasingly sophisticated and outsourced student data collection practices. For example, the definition of educational record and PII likely would not include unconventional types of student data collected through EdTech, such as a lunch item choice or the subject of an email message. Courts rarely consider the question and largely determine what constitutes PII and educational record on a case-by-case basis.[26]
- **It's complicated.** The Department of Education's 2014 FERPA guidance outlined types of information that would fall within the PII and educational record definitions.[27] However, the Department's response to most questions regarding proper evaluation of FERPA – including what FERPA requires if PII is shared – was "it depends."[28] This is likely because FERPA's exceptions significantly complicate the analysis. The majority of EdTech providers arguably meet the "school official" exception because they are often under contract with a school to perform an institutional service or function. The Department acknowledges that FERPA's regulations are not bright-line rules, and therefore encourages schools to evaluate the terms and conditions of each EdTech contract to determine whether the contract is FERPA compliant.[29] The end result is often schools and EdTech companies failing to notice potential FERPA violations in their contracts[30], and FERPA's privacy-protective goals being undermined.[31]
- **Its enforcement actions are severe and limited.** FERPA only regulates schools, and therefore companies are technically not required to comply with the law's guidelines. The Department of Education can investigate an EdTech company, but can only sanction the school or school district for FERPA violations. Moreover, the only sanction available to the Department is denial of all federal funding to the school – which is likely why this penalty has yet to be used.[32]

---

[26] DALIA TOPELSON ET AL., PRIVACY AND CHILDREN'S DATA: AN OVERVIEW OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT AND THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT 2 (2013) ("A 'person acting for' the educational agency generally refers to agents of the school, such as teachers, administrators, and other school employees. The Supreme Court has also stated that a person cannot be 'acting for' an agency unless he or she also 'maintains' the record. Accordingly, peer-graded student papers and some student papers and tests that are briefly held for correction and grading alone are unlikely to be considered to be 'maintained' by an education institution or a person acting for an educational institution").

[27] U.S. DEPARTMENT OF EDUCATION PRIVACY TECHNICAL ASSISTANCE CENTER, PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 2-3 (2014)

[28] *Id.*

[29] *Id.*

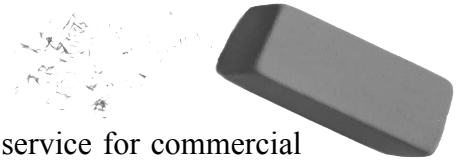
[30] JOEL R. REINDENBERG ET AL., PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS, Executive Summary (2013).

[31] Daniel Solove, *The Battle for Leadership in Education Privacy Law: Will California Seize the Throne?,* LINKED IN BLOG (Mar. 31, 2014), https://www.linkedin.com/today/post/article/20140331063530-2259773-the-battle-for-leadership-in-education-privacy-law-will-california-seize-the-throne?trk=nmp_rec_act_article_detail.

[32] *Id.; See also Family Policy Compliance Office: Court Cases,* ED.GOV, http://www2.ed.gov/policy/gen/guid/fpco/courtcases/index.html (last visited May 8, 2015). The Family Policy Compliance Office (FPCO) is charged with enforcing FERPA and PPRA on behalf of the Department. Its website lists only one FERPA violation action brought by the Department. The action was brought in 2002 and the Department received an injunction against the school.

Children's Online Privacy Protection Act ("COPPA")

COPPA regulates commercial websites and online services directed to children under 13 years old that collect, use, or disclose personal information from children, as well as general audience websites or online services with actual knowledge that they collect, use, or disclose personal information from children under 13.[33] It also applies to websites and services that know they are collecting information directly from users of a service or website directed to children. COPPA *does not* extend to sites and services that only collect information *about* children; this means a site or service would not be covered if it receives its data on children from adults (for example from a parent, teacher or school). If a website or service is covered by COPPA, the law requires the operator to obtain verifiable parental consent prior to collecting or sharing the child's data. COPPA also allows schools to act as agents of parents to provide this consent in certain circumstances.[34]



Important terms

- **Operator:** Any person who operates a website or online service for commercial purposes and collects or maintains personal information from the users of this website or service.[35]
- **Child:** Any individual under 13 years old.[36]
- **Personal Information:** Individually identifiable information collected on a person, including name, social security number, address, email, telephone number or any other information the Federal Trade Commission ("FTC") determines could be used to contact the person.[37] Note that this is not identical to FERPA's definition of PII.[38]
- **Verifiable Parental Consent:** Any reasonable effort by an operator to both provide the parent with notice of, and receive consent for, its intention to collect, use or disclose information on the child.[39] It must be obtained prior to the operator collecting, using or disclosing a child's personal information. A school may provide consent on behalf of the parent when the operator is under contract with the school, and the collection and disclosure are for "the use and benefit of the school, and no other commercial purpose."[40] The scope of the school's authority to act on behalf of the parent is limited to the school context.

COPPA, while effective, cannot monitor EdTech alone

- Although COPPA helps ensure companies collect and use children's data responsibly, the law is limited only to sites or services that collect information

[33] *Complying With COPPA: Frequently Asked Questions,* FTC.GOV, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions (last visited May 22, 2015).
[34] *Id.*
[35] 15 U.S.C. §§6501-06.
[36] *Id.*
[37] *Id.*
[38] LEAH PLUNKETT ET AL., FRAMING THE LAW & POLICY PICTURE: A SNAPSHOT OF K-12 CLOUD-BASED ED TECH & STUDENT PRIVACY IN 2014 16 (2014).
[39] 15 U.S.C. §§6501-06.
[40] *Complying With COPPA: Frequently Asked Questions,* FTC.GOV, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions (last visited May 22, 2015).

from children under 13 years old, and not information provided by adults about these children. This means a site or service would not have to comply with the law if the information it collects on an under-13-year-old is only obtained from a parent, school, or presumably anyone 13 or older.

- The law does not regulate collection, use, or disclosure of data of 13-17 year olds. EdTech companies are therefore not subject to liability under COPPA if their services target children 13 years and older, which includes the majority of high school and some junior high school students. COPPA was not designed to be a student privacy law, and we are *not* advocating for extending COPPA's protections to 13+ year olds. However, the limits on COPPA's applicability emphasize the need for legislation that reaches EdTech companies beyond those subject to COPPA. This is especially important given the unique privacy concerns in the educational space versus the purely commercial space. For one, there's a stronger argument that creating targeted ads from a fifteen-year-old's visit to an online shopping site meets her reasonable expectation of privacy, than there is for generating those same ads from her tenth-grade math quiz. Secondly, students of all ages are often *required* to use EdTech to complete various tasks for school, such as standardized tests, homework, or in-class assignments, meaning there is much less user autonomy from the start. Federal legislation must be passed that reaches EdTech providers targeting K-12 students of any age.

Protection of Pupil Rights Amendment ("PPRA")

This law requires schools that receive funds from the US Department of Education to obtain written consent from parents prior to conducting any survey, test or evaluation that has the purpose of collecting sensitive information on a student. "Sensitive information" includes birthdate and mailing and email addresses, as well as political affiliations, mental health, sexual health and attitudes, and behavior assessments.[41] PPRA is not discussed as frequently as FEPRA and COPPA in the student privacy context, but may become increasingly relevant as EdTech evolves to streamline the process by which schools administer tests and surveys.

Section 5 of FTC Act

Pursuant to Section 5 of the FTC Act, the FTC has the authority to take action against companies engaged in "unfair or deceptive" business practices. Unfair or deceptive business practices are defined as those that (1) cause or are likely to cause substantial injury to consumers, (2) are not reasonably avoidable by consumers themselves and (3) are not outweighed by countervailing benefits to consumers or to competition.[42] If existing federal law does not evolve, Section 5 may be one of the few means of directly regulating EdTech providers. The FTC has received multiple Section 5 violation complaints against EdTech companies alleged to have engaged in unlawful business practices.[43] In May 2014, the agency's Consumer Protection Bureau wrote a letter to the court overseeing ConnectEDU's bankruptcy proceeding to argue that the EdTech company's proposed post-bankruptcy data sells would run afoul of Section 5 and the

[41] 20 U.S.C. § 1232h; 34 CFR Part 98.
[42] 15 U.S.C. Sec. 45(n).
[43] *See Student Privacy,* EPIC.ORG, https://epic.org/privacy/student/ (last visited May 22, 2015).

Bankruptcy code.[44] For some advocates this letter was a sign that the FTC would more aggressively pursue Section 5 violations against EdTech.[45] However, the FTC's response in this case was somewhat of an anomaly: the agency rarely brings Section 5 enforcement actions against EdTech companies, and it is unclear whether Section 5 will be enforced against EdTech with much frequency in the future. Additionally, Section 5 authority does not require certain day-to-day privacy-protective practices, nor was it intended to: Section 5 was primarily designed to respond to bad acts.

Reform Efforts

There have been numerous efforts to reform EdTech student data collection practices over the past year and a half, including legislative and policy advocacy, consumer education and voluntary industry regulation.

State Action

Over 170 state student privacy bills were introduced in the first four months of 2015.[46] A number of state student privacy bills and laws that cropped up in previous years only regulated educational institutions. For example, Oklahoma's 2013 "Student DATA Act," which was imitated by numerous bills proposed in other states, only regulates the state department of education and school districts. It requires the department of education to establish a public facing inventory of the types of student data collected by the department, develop policies regarding access to student data, comply with federal law security mandates, and limit transfer of student data to entities outside of Oklahoma.[47] The law was intended to comprehensively address mass collection of student data by EdTech platforms. However, by limiting its applicability to the state department of education and school districts, the law ultimately allows companies to avoid liability for their own collection, use, and sharing of student data.

The Student Online Personal Information Protection Act ("SOPIPA"), California's student privacy legislation passed in September 2014, is a noteworthy departure from these types of laws. SOPIPA prohibits K-12 education online services and mobile applications from (1) engaging in targeted advertising to students or their families; (2) using information collected on students to create advertising profiles; (3) selling information on a student; or (4) disclosing students' personal information except under

[44] Press Release, Federal Trade Commission, FTC Seeks Protection for Students' Personal Information in Education Technology Company ConnectEdu's Bankruptcy Proceeding, May 23, 2014 (on file with author). http://www.ftc.gov/news-events/press-releases/2014/05/ftc-seeks-protection-students-personal-information-education?utm_source=govdelivery.

[45] Michele Molnar, *FTC Acts to Protect Student Data in Proposed Ed-Tech Bankruptcy Sale*, EDUCATION WEEK BLOG (May 23, 2014, 5:13 PM), http://blogs.edweek.org/edweek/marketplacek12/2014/05/ftc_acts_to_protect_student_data_in_proposed_ed-tech_bankruptcy_sale.html.

[46] Rachel Anderson, *EdData Privacy Update: 5/22/2015,* DATA QUALITY CAMPAIGN BLOG (May 22, 2015), http://www.dataqualitycampaign.org/blog/2015/5/eddata-privacy-update-5-22-2015/.

[47] *Oklahoma's New Student DATA Act Sets Guidelines, Protections,* DATA QUALITY CAMPAIGN BLOG (Sept. 26, 2013), http://www.dataqualitycampaign.org/blog/2013/09/oklahomas-new-student-data-act-sets-guidelines-protections/.

limited circumstances.[48] At least 10 states, including Florida, Illinois, Massachusetts, Minnesota, and Georgia have introduced SOPIPA-type bills in 2015. It should be noted that SOPIPA *does not* include data minimization language, although an earlier version of the law incorporated such provisions.[49] Although we support SOPIPA generally, we believe this omission limits its effectiveness, and hope other states will take the lead on passing laws that both extend to EdTech directly *and* require data minimization.

Federal action

A number of student privacy federal legislative proposals have made headlines in 2015. Some of these proposals have been formally introduced and others are still awaiting introduction. Below are details on bills that have been introduced:

- **Student Digital Privacy and Parental Rights Act.** Representatives Luke Messer and Jared Polis introduced a bipartisan effort, the "Student Digital Privacy and Parental Rights Act", in April 2015.[50] The bill sets sensible baseline rules for K-12 websites, online services, and apps to protect the privacy and security of students' personal information. These include prohibiting targeted advertising, sale and creation of personal profiles except for school purposes; prohibiting disclosure of students' personal data to third parties except in limited circumstances; requiring third party recipients to comply with robust data protection standards; requiring companies to delete student data after 45 days at the school's request or the parent's request; purging student data after a year unless a school or parent has directed the company to maintain the data; and giving the FTC rulemaking and enforcement authority. The bill still permits use of EdTech for personalized and adaptive student learning purposes. It also permits use of aggregated, de-identified information for research and product improvement, and allows schools to retain data if retention is for an educational or administrative purpose. This bill strikes an appropriate balance so students can benefit from online learning products, while minimizing potential harms associated with third party data sharing.
- **Protecting Student Privacy Act.** Senators Ed Markey and Orrin Hatch reintroduced a bipartisan bill in May 2015, the "Protecting Student Privacy Act" that would amend FERPA.[51] The bill prohibits the use of PII for targeted advertising, mandates EdTech security policies, and limits the information schools may distribute to third parties.[52] The bill also gives parents the right to review and demand correction of incorrect or misleading information on a student, and requires companies to destroy data after it has been used for its intended educational purpose.[53] While this bill would enhance protections for students and parents in many respects, we are concerned that the bill does not

[48] Alex Bradshaw, *California Takes Meaningful Step Toward Shoring Up Student Privacy,* CDT BLOG (Sept. 30, 2014), https://cdt.org/blog/california-takes-meaningful-step-toward-shoring-up-student-privacy/.
[49] *Id.*
[50] Press Release, Representative Jared Polis, Messer, Polis, Introduce Landmark Bill to Protect Student Data Privacy, Apr. 29, 2015 (on file with author). http://polis.house.gov/news/documentsingle.aspx?DocumentID=397810.
[51] *See* Press Release, Senator Edward Markey, Sens. Markey & Hatch Reintroduce Bipartisan Legislation to Protect Student Privacy, May 13, 2015 (on file with author). http://www.markey.senate.gov/news/press-releases/sens-markey-and-hatch-reintroduce-bipartisan-legislation-to-protect-student-privacy.
[52] *Id.*
[53] *Id.*

seek to expand the definition of "educational record." Given that private companies collect vast amounts of information on students that arguably would not be considered an educational record – such as performance on online tutorials, geolocation data, and website visits – this creates a loophole in the bill's protections.[54]

- **Student Privacy Protection Act.** Senator David Vitter introduced a FERPA amendment proposal, the "Student Privacy Protection Act," in May 2015.[55] The bill appears to prohibit all third-party sharing without parental consent, including sharing with contractors or other parties under the direct control of the school. The bill also prohibits sharing student data with SLDS unless the data is de-identified, aggregated, and anonymized. As noted earlier, sharing student data with third parties may be acceptable in certain circumstances and it would be impractical to obtain user consent for all disclosures to third parties. We are therefore concerned that these provisions in Senator Vitter's bill are overly restrictive and may hinder benefits students could receive from use of EdTech.

In addition to bills already introduced in Congress, there are federal legislative proposals circulating among stakeholders:

- Representatives Bobby Scott and John Kline shared a discussion draft bill in April 2015 that would amend FERPA in a number of respects, including expanding the definition of "educational record", broadening the penalties available to the Department of Education to enforce FERPA and providing opt-in controls for parents for particular data sets.[56]
- In January 2015, President Obama announced a legislative proposal, the Student Digital Privacy Act, which would work in conjunction with FERPA to regulate collection of students' data. The Act – modeled closely after California's SOPIPA – would directly reach EdTech providers and limit sharing of student data with third parties for marketing and/or advertising purposes.[57] The text of the Student Digital Privacy Act was never made public.

Industry Action

In October 2014, the Software & Information Industry Association ("SIIA") and the Future of Privacy Forum released a Student Privacy Pledge, a voluntary industry pledge to comply with certain student privacy and security commitments.[58] The Pledge requires signatories to "not sell student information or behaviorally target advertising, use data for authorized educational purposes only, and not change privacy policies without notice."[59] The Pledge also requires these companies to "enforce strict limits on data retention,

---

[54] *Id.*

[55] Press Release, Senator David Viter, Vitter Introduces Student Privacy Protection Act, May 14, 2015 (on file with author). http://www.vitter.senate.gov/newsroom/press/vitter-introduces-student-privacy-protection-act.

[56] Benjamin Harold, *Major FERPA Overhaul Under Consideration in U.S. House,* EDWEEK DIGITAL EDUCATION BLOG (Apr. 7, 2015, 2:27 PM), http://blogs.edweek.org/edweek/DigitalEducation/2015/04/ferpa_overhaul_US_House.html.

[57] Alex Bradshaw, *President Obama Announces Student Privacy Legislative Proposal,* CDT BLOG (Jan. 12, 2015), https://cdt.org/blog/president-obama-announces-student-privacy-legislative-proposal/.

[58] *See Student Privacy Pledge,* STUDENTPRIVACYPLEDGE.ORG, http://studentprivacypledge.org (last visited May 26, 2015).

[59] *Id.*

support parental access to and correction of errors in their child(ren)'s records, provide comprehensive security standards, and be transparent about collection and use of data."[60] If a signatory violates one of the Pledge's commitments the FTC could bring a Section 5 complaint against it. However, there is no specific enforcement provision in the Pledge, nor is there an enforcement regime (similar to a Better Business Bureau) behind the effort that monitors compliance, and takes disciplinary action or informs the FTC when a company is not compliant. This is concerning because there is no guarantee that the FTC will be notified of noncompliance in order to take action against a signatory.

Solutions

CDT believes in the power of technology to enhance the classroom. However realizing the full potential of EdTech requires protecting students' rights to privacy and data security. Given this, the following should be priorities for schools, legislators and EdTech companies:

The Family Educational Rights and Privacy Act (FERPA) should be amended.
As discussed earlier, the law's definition of "educational record" must be expanded to include information collected by EdTech that does not fall within the current definition. Furthermore, the Department of Education should be able to apply graduated penalties against educational institutions found to have violated the law. This would give the Department more practical means of enforcing the law, and better incentivize schools to ensure their EdTech contracts are FERPA-compliant (because the Department would be more likely to penalize the school for a violation).

The current federal legislative framework must be updated and/or augmented to directly reach EdTech providers.
As noted, COPPA's mandates are limited to companies that target children under 13 years old, which omits many middle school students and most high school students. EdTech is arguably used with more frequency in middle and high schools, and it is critical that laws are in place that extend to companies targeting these student populations. Furthermore, while Section 5 authority may allow for the FTC to file administrative complaints against an EdTech provider in certain circumstances, it is unclear whether the agency considers EdTech data collection practices complained of as "unfair or deceptive" because the agency has taken little action to enforce Section 5 against EdTech companies as a result of complaints. Federal legislation should be passed that broadens the FTC's authority to directly reach EdTech, and explicitly prohibits certain data collection, use, and sharing practices that go beyond schools' authorizations and students' and parents' reasonable expectations. Furthermore, the law should be a floor and not a ceiling: a federal EdTech regulatory effort should only preempt state laws to the extent that they are weaker than the federal standard. This will allow for states to innovate on student privacy to afford their students enhanced privacy protections.

[60] *Id.*

Data deletion and minimization requirements should be included in legislation, as well as industry and school policies.

In its January 2015 "Internet of Things" report, the FTC identified a number of data collection practices companies should adopt to protect consumer privacy and security. Data minimization was among these recommendations.[61] Data minimization involves limiting both the amount of consumer data collected on the front end, and how long this data is retained by the company. The report notes that minimization addresses two risks: "First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations."[62]

Companies have the capacity to collect and retain large amounts of highly sensitive data about students, such as test results, social and emotional assessments, and physical health information.[63] While this data may be useful for analysis of a student or educational program, students and their parents should be able to trust that this data will not be kept in perpetuity for any and all purposes. At the very least, eligible students and parents should have the ability to request deletion of certain data after they graduate or after it is no longer being used for an educational purpose. Companies should also be expected to purge data at some point, even absent a deletion request.

Unfortunately, data minimization requirements are absent in a lot of existing law. FERPA does afford parents and eligible students the right to access and correct certain information kept in an educational record; however, school officials (most EdTech providers) are not under an obligation to destroy data after a certain point, nor do parents or students have the right to request deletion of certain data.[64] Furthermore, some of the strongest state laws – such as California's SOPIPA – lack data minimization requirements.[65]

Data collection and retention must be purposeful. Companies and schools that implement thoughtful processes on the front end for determining what data to collect, and how long

---

[61] Alex Bradshaw, *FTC Says Privacy Still Matters on "Internet of Things",* CDT BLOG (Jan. 30, 2015), https://cdt.org/blog/ftc-says-privacy-still-matters-on-internet-of-things/.

[62] FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. These risks are undoubtedly present in the education context. Approximately 30 institutions of higher education experienced data breaches in 2014 alone. Five of these hacks were larger than the 2014 Sony Entertainment data breach. Information stolen included, among other data, students' bank account information, social security numbers and drivers license numbers. University of Maryland's hack exposed information on over 300,000 students, faculty and staff. The database broken into contained information on everyone who'd received a university ID since 1998. *See* Kyle McCarthy, *5 Colleges with Data Breaches Larger than Sony's in 2014,* HUFFINGTON POST BLOG (Jan. 15, 2015), http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html.

[63] *See* ISAAC MEISTER & ALICIA SOLOW-NEIDERMAN, K-12 EDTECH CLOUD SERVICE INVENTORY 2 (2014).

[64] 20 U.S.C. §1232g, 30 C.F.R. §99.7 §99.37.

[65] Alex Bradshaw, *California Takes Meaningful Step Toward Shoring Up Student Privacy,* CDT BLOG (Sept. 30, 2014), https://cdt.org/blog/california-takes-meaningful-step-toward-shoring-up-student-privacy/.

to keep it, are arguably less susceptible to data breaches, as well as the reputational damage and loss of student trust that accompany a breach. For this reason, companies, schools, and legislators should embrace data minimization when determining how best to protect students' personal information.

Sharing limitations should be included in legislation, as well as industry and school policies.

It is critical that the number of entities that have access to student data is appropriately scoped. Although sharing student data with third parties may be appropriate in certain circumstances – such when it's being used by the third party to provide the student with health services or additional academic support – some sharing of student data arguably would not meet students' reasonable expectation of privacy. Students have complained of these third party uses in recent years, even going so far as to bring lawsuits against companies that used their data for targeted advertising.[66]

Current federal law allows for some third-party data sharing, and it would be impractical to prohibit all sharing or require user consent in all circumstances. However, data sharing should only occur when it is for a valid educational purpose. There should not, for example, be a blanket exception to a law's disclosure limitations and consent requirements for all researchers. Some research may have nothing to do with education, and students would not reasonably expect that every element of their performance will be freely shared with these researchers in the name of "Big Data." In such cases, parents and students should have control over whether their data is shared.

Federal legislation should incentivize companies and schools to appropriately scope student data sharing. Moreover, EdTech should consider implementing tactics such as de-identification (although we note de-identification is not a silver bullet[67]) that would further secure students' privacy once their data is shared. This is in line with FERPA regulations that allow for the release of a student's PII without parental consent if the data is de-identified.[68] Additionally, students and parents should be notified of data collection practices and given the opportunity to "opt-in" or "opt-out" of practices that exceed reasonable expectations. Companies should make a good-faith effort to determine when these controls are appropriate. Some data collection may require clear opt-in because it's sensitive or out of context. Other information may be collected automatically, but consumers should have the ability to opt out of secondary data retention or transfer. Some data collection consumers likely shouldn't have control over because it is necessary for operation of the device.

[66] *For more on these allegations see Student Privacy,* EPIC.ORG, https://epic.org/privacy/student/ (last visited May 22, 2015).
[67] Natasha Singer, *With a Few Bits of Data Researchers Identify 'Anonymous' People*, N.Y. TIMES (Jan. 29, 2015), http://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/?_r=0.
[68] 30 C.F.R. §99.31.

Final Thoughts and Areas for Further Action

Adoption of these policy recommendations will undoubtedly shore up student privacy. However, it is important that these reform efforts are used to enhance the privacy of *all* students. The current student privacy debate, while thoughtful and engaging, often omits consideration of two groups: postsecondary school students and underprivileged K-12 students. Postsecondary school students have unique data privacy concerns and are equally (if not more) at risk of being victimized by data misuse as K-12 students. While K-12 school data hacks are rare (or rarely reported), news of college and university data breaches is common. As noted, over 30 university data breaches occurred in 2014 alone. Postsecondary schools collect highly sensitive student data, (social security numbers, bank account and loan information, healthcare history, and the like), however, it appears some schools lack the data protection resources that should accompany such collection. This threatens students' future financial, professional, and personal well being. Student privacy is also a civil rights concern; we increasingly read stories of "Big Data" fostering negative profiling and discrimination. This puts disadvantaged students (such as low-income, minority, and LGBT students of all education levels) in an especially vulnerable position. All students – especially those disproportionately subject to negative profiling *offline* – must be able to trust that the services they interact with online will not perpetuate such discrimination. We must broaden the debate to include these groups and swiftly put policies in place to advance all students' privacy.

For more information contact:

Alex Bradshaw
Center for Democracy & Technology
202.407.8822
alex@cdt.org