Spying on Students

SCHOOL-ISSUED DEVICES AND STUDENT PRIVACY

Frida Alim, Bridge Fellow

Nate Cardozo, Senior Staff Attorney

Gennie Gebhart, Researcher

Karen Gullo, Media Relations Analyst

Amul Kalia, Analyst

April 13, 2017

Authors: Frida Alim, Nate Cardozo, Gennie Gebhart, Karen Gullo, Amul Kalia
With assistance from: Sophia Cope, Hugh D'Andrade, Jeremy Gillula, Rainey Reitman

A publication of the Electronic Frontier Foundation, 2017.

Table of Contents

Executive Summary

Students and their families are backed into a corner. As students across the United States are handed school-issued laptops and signed up for educational cloud services, the way the educational system treats the privacy of students is undergoing profound changes—often without their parents' notice or consent, and usually without a real choice to opt out of privacy-invading technology.

Students are using technology in the classroom at an unprecedented rate. One-third of all K-12 students in U.S. schools use school-issued devices.[1] Google Chromebooks account for about half of those machines.[2] Across the U.S., more than 30 million students, teachers, and administrators use Google's G Suite for Education (formerly known as Google Apps for Education), and that number is rapidly growing.[3]

Student laptops and educational services are often available for a steeply reduced price, and are sometimes even free. However, they come with real costs and unresolved ethical questions.[4] Throughout EFF's investigation over the past two years, we have found that educational technology services often collect far more information on kids than is necessary and store this information indefinitely. This privacy-implicating information goes beyond personally identifying information (PII) like name and date of birth, and can include browsing history, search terms, location data, contact lists, and behavioral information. Some programs upload this student data to the cloud automatically and by default. All of this often happens without the awareness or consent of students and their families.

In short, technology providers are spying on students—and school districts, which often provide inadequate privacy policies or no privacy policy at all, are unwittingly helping them do it.

Since 2015, EFF has been taking a closer look at whether and how educational technology (or "ed tech") companies are protecting students' privacy and their data. This paper presents what we have observed and learned about student privacy in the course of our investigation. We aim to more precisely define the problems and issues around student privacy as they affect real students and their families, and to give stakeholders—including parents, students, administrators, and teachers—concrete steps they can take to advocate for student privacy in their own communities.

After an **introduction** to EFF's approach to student privacy, we turn to our analysis.

In **Part 1**, we report on the results of a large-scale survey and interview study we conducted throughout 2016. In particular, we found that in an alarming number of cases, ed tech suffered from:

- **Lack of transparency.** Schools issued devices to students without their parents' knowledge and consent. Parents were kept in the dark about what apps their kids were required to use and what data was being collected.
- **Investigative burdens.** With no notice or help from schools, the investigative burden fell on parents and even students to understand the privacy implications of the technology they were using.
- **Data concerns**. Parents had extensive concerns about student data collection, retention, and sharing. We investigated the 152 ed tech services that survey respondents reported were in use in classrooms in their community, and found that their privacy policies were lacking in encryption, data retention, and data sharing policies.
- **Lack of choice.** Parents who sought to opt their children out of device or software use faced many hurdles, particularly those without the resources to provide their own alternatives.
- **Overreliance on "privacy by policy."** School staff generally relied on the privacy policies of ed tech companies to ensure student data protection. Parents and students, on the other hand, wanted concrete evidence that student data was protected in practice as well as in policy.
- **Need for digital privacy training and education.** Both students and teachers voiced a desire for better training in privacy-conscious technology use.

The data we collected on the experiences, perceptions, and concerns of stakeholders across the country highlights the need for ed tech companies to take seriously the privacy concerns of students, parents, teachers, and administrators.

In **Part 2**, we provide in-depth analysis of ed tech's legal and policy framework in the U.S. State and federal laws that are supposed to protect student privacy have not kept up with ed tech's rapid growth. We address:

- **Industry self-regulation.** The Student Privacy Pledge, enforced by the FTC and voluntarily signed by ed tech companies, features glaring loopholes in its definitions of what constitutes "student information" and "educational service providers."
- **Federal law.** We provide legal analysis of key federal laws the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), highlighting major flaws in each law—namely, FERPA's "school official" loophole and questions about parental consent in COPPA.
- **State law.** As states bring forward more and more student privacy legislation, three have stood out: California, Colorado, and Connecticut. We describe each state's current legislation and the ways in which they each take unique steps to protect student data, provide resources to school districts, and rein in ed tech companies.

In **Part 3**, we turn our analysis into a call for action and present our recommendations for: school administrators, teachers, librarians, system administrators, parents, students, and ed tech companies themselves.

Finally, we **conclude** by bringing our survey reporting, legal analysis, and recommendations together to briefly state the key problems and issues surrounding K-12 digital student privacy in the U.S.

Want to learn more about digital privacy? Readers of this paper may be interested in digital privacy in general, not just in the educational context. If so, check out EFF's privacy work[5] and our Surveillance Self-Defense guide.[6]

Introduction

In December 2015, the Electronic Frontier Foundation started a campaign to raise awareness about the risks to student privacy when companies collect students' data. Since then, we have fought for the privacy and security of student data on multiple fronts. We launched a nationwide survey to learn how parents, students, teachers, and administrators experienced student privacy issues; we provided answers to questions about the legal and technological landscape of ed tech; we filed a complaint with the Federal Trade Commission regarding the data collection practices of Google's G Suite for Education; and we created a wealth of resources for parents, students, and school staff.

While numerous and complex dynamics shape the ed tech and student privacy landscape, we have focused on only one: the threat to K-12 students and their privacy posed by school-issued devices and ed tech platforms.

Our narrow focus interacts with broader driving forces in ed tech. While we cannot address them all, they provide valuable context and deserve acknowledgement. For example, ed tech gives disabled students new learning opportunities and is indispensable in special learning environments. Further, technology in schools gives states opportunities to understand student performance over time and be accountable for the effects of educational initiatives.

Ed tech's growth is also closely tied to newer market and policy forces. Valued at over $8 billion,[7] the educational technology sector in the U.S. has been described as "the world's most data-mineable industry by far."[8] As companies race to produce and capture more student data, the U.S. Department of Education has encouraged schools to use "big data" analysis to improve assessment and educational innovation.[9] Common Core's computerized testing requirements and other developments in education policy have also increasingly driven ed tech adoption forward.[10] In the midst of these changing requirements, underfunded schools' lack of resources can make them particularly

susceptible to offers of free devices and educational software from large ed tech companies.[11]

While governments, schools, and industry shape the ed tech space, sensitive student data is caught in the middle—and this is where EFF places its focus. As ed tech growth outpaces legal and ethical understanding of its privacy implications, we risk placing students under silent yet pervasive surveillance that chills their creative expression both in and outside the classroom, and tracks their online behavior before they are old enough to understand its consequences.

In the long term, protecting student privacy means protecting children from surveillance culture at school and at home. The constant surveillance in which ed tech results can warp children's privacy expectations, lead them to self-censor, and limit their creativity.[12] A surveillance environment built by trusted teachers and educators will socialize children to ignore and even accept the routine collection, retention, and sale of their personal information.[13] Ed tech unchecked threatens to normalize the next generation to a digital world in which users hand over data without question in return for free services—a world that is less private not just by default, but by design.

In this white paper, we aim to paint a vivid picture of what it looks like when the privacy policies and practices of ed tech companies interact with real students and their families. We hope to provide a more holistic understanding of not only the legal and policy framework in which ed tech is growing, but also the real-life privacy impact that educational technologies have on the individuals tasked with deploying, using, and understanding them.

Part 1: Survey Results

Student privacy is about more than data collection and legal protections; it is about real students and their families. What does it look like in real communities when ed tech company policies and state and federal legislation interact with students and their data?

In late 2015, we launched an online survey to collect information and stories from real people about their experiences with student privacy. Over the next year, we heard from over 1000 students, parents, students, teachers, administrators, and other stakeholders about the student privacy experiences and challenges they had encountered in their own communities.

Eight main trends emerged from survey responses and interviews. We found that (1) parents and students experienced a lack of transparency from schools, with parents reporting little or no disclosure of what technology their students were using in the classroom. (2) This lack of notice from schools put the investigative burden on parents and even students to address (3) their extensive concerns about student data collection,

retention, and sharing. And their concerns were well-founded; (4) we investigated the 152 ed tech services reported as in use in classrooms, and found troubling trends in their privacy policies regarding lack of encryption, opaque data retention practices, and inadequate data aggregation and de-identification. (5) Parents who chose to withdraw their students from certain technology use were often met with few choices and insurmountable hurdles. (6) Stakeholders' lack of trust in policies and legislation highlighted the fact that "privacy by policy" is not good enough, and must be backed up by concrete technological safeguards. To successfully execute any privacy-protecting policies and safeguards, (7) teachers need better training in technology and digital privacy. Finally, (8) students need enhanced digital literacy education to take control of their privacy in the classroom.

Below we describe our methods and the characteristics of our respondents and their schools before delving into these eight findings in more detail.

Methods

We distributed an online survey on student privacy via EFF's website, blog posts, the EFFector newsletter, and social media between December 2015 and January 2017. From there, the survey "snowballed" out, with respondents encouraged to share the survey link with others.

The survey asked about respondents' location; what kind of devices their district was issuing, if any; whether devices were issued on a one-to-one basis; whether devices stayed at school or could go home with students; what grade levels were issued devices; what ed tech programs, apps, or software the school was using, if any; how parents were notified about data collection, if at all; whether parents could opt their children out of technology use; and respondents' self-reported level of concern about student privacy. Finally, the survey concluded with an open-ended question requesting any additional information respondents wanted to share, from which we collected the quotes that appear throughout the findings below. (See full survey in Appendix.)

After the survey concluded, we selected several respondents for longer, in-depth interviews. We drew from the approximately one-third of survey respondents who provided their contact information and indicated that they were willing to be contacted by EFF. These interviews appear throughout our findings below as pull-out case studies, each digging into one individual's experience with a particular aspect of student privacy.

Because we used a "snowball" sample and targeted interviews, our findings cannot be considered generalizable or representative. Instead, the survey results and case studies are meant to shed light on the human side of student privacy: the attitudes, perceptions, and types of individual concern and awareness that shape action around student privacy on the ground.

Respondents and Overall Trends

We heard from 1034 survey respondents from several stakeholder groups:

- 468 students
- 393 parents
- 69 teachers, including librarians and other teaching staff
- 31 school administrators, including system administrators and other general staff
- 73 other community members

Students and parents make up the majority of our respondents at about 83 percent. Therefore, while we report on stakeholders across the spectrum, the survey puts us in a position to make the strongest assertions about students and parents.

Respondents came from 45 states, Washington D.C., and Guam, as well as from 17 other countries around the world. While this paper focuses on U.S. policy and practices, the geographical variety of survey responses serves as a reminder that ed tech companies—along with the services they offer and the privacy issues they pose—are global.

Google devices and platforms dominated survey responses. Half of respondents reported Chromebook use in their school or district, followed by iPads (32%) and Microsoft Surface tablets (3%). G Suite for Education was also the most popular platform, with 63 percent of respondents reporting G Suite use in their district. Note that these numbers do not necessarily reflect the school adoption of these ed tech products and services nationally. They simply mean that we heard the most about Google, and therefore are in a position to report the most stakeholder experiences with its products.

Among respondents, 45 percent reported that their schools or districts did not provide parents with written disclosure about ed tech and data collection, and 31 percent were not sure if such disclosure was provided. Further, 32 percent of all respondents reported that their schools or districts did not offer opt-out—that is, non-technological classroom alternatives for families who did not want students using certain technology—and 37 percent were not sure if opt-out was available. Again, these numbers do not describe school policy patterns across the country. Instead, these numbers characterize the environments of our respondents, who overwhelmingly experienced a lack of transparency and lack of choice with regard to student privacy.

Findings

We organize our findings into eight key takeaways, supported by quotes and statistics from the survey and in-depth case studies from subsequent interviews.

1. Lack of Transparency

The notice and disclosure process is broken. Parents who responded to the survey were overwhelmingly not notified when schools started using new softwares and devices,

created email accounts for students, or posted pictures of students on school or teacher social media pages.

One parent in a Maryland public school wrote:

We were given no information about our first-grader receiving a device—a tablet—this year. And when we ask questions, there is little information given at every level.

Even students took note of this, with one student observing that their Google account was "*provided suddenly without any notice*."

Teachers also had accounts created for them without notice or consent. One teacher wrote:

Staff and student details—that is, full names and school email addresses—were passed to Google to create individual logins without consent from staff. I'm not sure about consent from parents.

Sometimes, parents did not receive any information about ed tech use until after the technology had already been implemented and was in active classroom use. A parent in a California public school described how and when they were notified:

The specifics of the technology our children would use were not provided until back-to-school night, where the teacher emphasized the Chromebooks' value for individualized instruction.

These respondents are not alone. Survey trends regarding written disclosure of school practices and policies show that a majority of parents found themselves in the dark. Twenty-three percent of parents did not know whether or not they had received written disclosure about their school's ed tech practices, and 57 percent were sure they had not. That adds up to 80 percent of surveyed parents who did not have clear, readily accessible disclosure, suggesting a breakdown of communication between schools and parents.

2. The Investigative Burden

As a result of these failures in communication, the burden of investigating ed tech and its effect on privacy fell on parents and even students.

With awareness of technology in the classroom but without details, parents launched often exhaustive investigations of how their children were using ed tech. A North Carolina charter school parent described a months-long effort to obtain a comprehensive

Case Study: A California Parent Caught Off-Guard by Chromebooks

Katherine W. was seven years old, in the third grade, when her teacher first issued Google Chromebooks to the class. Katherine's father, Jeff, was concerned. Jeff feared that Chromebooks and G Suite for Education use might come at the cost of his daughter's privacy. He negotiated with his daughter's teacher so she could use a different computer and not have to use a Google account. But as third grade came to a close, the district made clear that there would be no exception made the next year.

Under the Family Educational Rights and Privacy Act (FERPA), the data that students often use to log into Google services—like name, student number, and birthday—can't be shared with third parties—including Google—without written parental consent.

But the district never sought written consent from Jeff or his wife. The district provided no details about the types of devices students would be required to use or the data that would be collected on students. Rather than allowing Jeff to sign his daughter up for the Chromebook program, the district consented on his behalf, making the device mandatory for Katherine—with no ability to opt out. This means that Katherine is required by the school to use Google with a personalized Google account, and Google can create a profile of her—that is, a dossier of information that vendors collect on users for advertising, market research, or other purposes—and use it for commercial purposes the moment she clicks away from G Suite for Education.

Jeff went through several emails and a tense meeting before the district agreed to provide Katherine with a non-Google option for fourth grade—but once again declared that such an accommodation would not be possible for fifth grade.

That's when EFF reached out to the district. Our legal team drafted a letter to the district to outline the privacy concerns associated with school-issued Chromebooks. The letter urged the district to permit "all students—if their parents so decide—to use alternative devices, software, and websites, for the upcoming school year and every year."

For Jeff, the biggest concern isn't just the data Google collects on students. It's the long-term ramifications for children who are taught to hand over data to Google without question.

As Jeff explained it, "In the end, Google is an advertising company. They sell ads, they track information on folks. And we're not comfortable with our daughter getting forced into that at such an early age, when she doesn't know any better."

list of the software, programs, and apps her child was using in school:

I have never received any written policy about how many apps the school uses and how they collect student data. The district maintains a website for parents to obtain information regarding technology in the classroom, but I have not found anything there about student privacy. When we asked for the apps that the school was using, we were hoping to see in writing what they're using. Instead, we got a short, verbal list—but when we look at our son's iPad, we see a lot more programs than what they told us about. What we want is a comprehensive snapshot of what technology experiences our son is having, especially if he has to log in to use them.

Many parents' efforts were stymied before they could get that far. Parents described confusing procedures around student privacy in their schools and districts. Multiple parents said there was "*no information available*" about data collection or student privacy, with a Connecticut parent adding:

The school was vague about what info was collected. It isn't clear who to speak with about the program and concerns.

In some cases, students took the investigation into their own hands. A student in a California private school described their efforts to find out what was installed on school-issued iPads:

I'm privacy-conscious, and I only know what I know due to reading through agreements and manually inspecting the install certificates on our iPads.

Another student in California, this one at a public school, went online to find privacy policies:

The companies providing the online services list privacy policies on their websites, but these policies are not shared directly with us or our parents.

The impetus should be on schools and ed tech companies themselves, not the parents and students on whom the technology is imposed, to be transparent about what technologies are being used in the classroom, what privacy policies govern them, and what privacy implications they may carry. As it stands, parents were on their own to find the information they needed to protect their children and advocate for their privacy.

3. Parent Concerns About Data Collection and Use

When parents' questions went unanswered, they were left with serious data concerns, particularly when devices and ed tech programs came home with students. Parents who responded to the survey were particularly concerned about personally identifiable information (PII) that could be used to identify a specific student, such as first/last name, birth date, student ID, graduation date, address, etc.

One Utah public school parent summed up a range of concerns:

Schools should not require students to use tools that involuntarily, or without express parental permission, collect data on students. This includes internal processing of data in order to "improve products," understanding user behavior to promote advertising, and sharing data with third parties.

A parent from a Maryland public school had suspicions about data collection, retention, and eventual use by ed tech companies:

They are collecting and storing data to be used against my child in the future, creating a profile before he can intellectually understand the consequences of his searches and digital behavior.

Parents were also conscious of the possibility that their children's data would be shared, sold, or otherwise commodified in the "*untapped industry of selling students' information for advertising and profiling*." The details were generally unclear, as school privacy policies said "*not a word about how our kids' learning is essentially becoming Google's data*." One Maryland parent wrote:

The school system does not even acknowledge that our child's data is being collected and possibly sold.

Within schools themselves, respondents observed practices that threatened to reveal students' PII on a smaller scale. Poor login and password management practices using PII were of particular concern. One California public school used students' birthdates as passwords. According to another parent:

The passwords are defaulted to student ID. Students are not allowed to change these passwords, and they have received emails stating that students are to stop attempting to change passwords. The student ID numbers are printed, unredacted, on schedules handed out to students and, per my child, "follow a pattern that is easily guessed."

When students came home with their school-issued devices and online homework, parents' data concerns extended from students' data to the family's home networks and devices. In addition to imposing surveillance on students at home as well as in the classroom,[14] ed tech had the potential to make other members of the household feel vulnerable. One public school parent in Pennsylvania wrote about their student accessing ed tech services on a personal device:

I have no idea how to find out the extent of information they [ed tech providers] have access to on our personal computers.

Another parent in a Virginia public school was concerned about their student using a school-issued device at home:

The students are required to use the laptops at home for assignments, but that could expose our home networks to the school system.

Parents' concerns above highlight the extent to which student privacy violations may go beyond the classroom. Student data—or, more broadly, data collected on students in the course of educational activities at school, at home, and elsewhere—may interact with advertising, drive inferences and profiles about individual students, or be shared with third parties.

4. Ed Tech Services Lacking Standard Privacy Precautions

All stakeholders—students, parents, teachers, administrators, and other staff alike—faced an overwhelming number and range of ed tech apps, softwares, programs, and services.

Survey respondents reported 152 distinct apps, software, and services in use in their schools' or districts' classrooms (see full list in Appendix). We investigated every service's privacy policy—particularly practices in data retention, encryption, and de-identification and aggregation—and they exhibited concerning trends.[15]

Privacy policies
Of the 152 ed tech services reported to us, only 118 had published privacy policies online. Some applications note that schools may implement their own privacy policies to govern personal data submitted to the services by student users.

Data retention
Of the 118 privacy policies, 78 mention data retention practices. Few privacy policies address deletion of data after periods of inactivity, which would allow the applications to retain information even after students graduate. We found a range of specific practices here, including:

- Evernote maintains copies of information on the service's back-up server for up to a year after a user has requested that the data be deleted.
- For Haiku Learning, the schools, rather than individual students, retain the authority and ability to delete information from the application.
- Lexia Learning requires that students and parents contact the school administrator to facilitate requests to access, change, or delete personal information. Absent a request from a school administrator, Lexia retains the information for as long as the account is active or as needed for Lexia to provide services.
- Storyboard retains student data for up to four years of inactivity.

Encryption
Of the 118 privacy policies we examined, only 46 state that the vendor uses encryption. That means that only about 30 percent of the 152 services reported to us make any

statement about encryption. This lines up with previous reports on the lack of support for encryption in ed tech.[16]

Encryption is crucial to protect sensitive student information from eavesdropping, and encrypting data in transit is widely recognized as absolutely necessary for even a minimal level of security. However, among the policies we investigated, encryption was most often only mentioned in connection with protecting the billing information of clients. Generally, policies gave little information about encryption protocols or which data a given service encrypts.

De-identification and aggregation
Of the 118 privacy policies, only 51 mention de-identification or aggregation of user data. Data de-identification is almost exclusively mentioned in connection with providing information to third parties about their services, reporting on student performance in districts, or analyzing use of their services.

5. Barriers to Opt-Out

Parents who acted on their concerns to opt their children out of technology were met with multiple hurdles. 40 percent of parents who responded to the survey did not know whether or not they could opt out of technology use in their school or district, and about 30 percent were sure they could not. That adds up to a whopping 70 percent of surveyed parents who did not perceive options or alternatives for their children's education.

Even in schools with opt-out policies on the books, families struggled to opt their children out of technology use. One parent from an Arizona private school wrote, simply:

Opt-out is possible in theory, but not in practice.

An Oregon public school student who investigated opt-out options on their own found a disconnect between the school's apparent willingness to accommodate and what options the school was actually prepared to provide in practice:

I personally spoke with the teachers at my school about technical judgments and hesitations I had. They were fully willing to allow me to use alternative means of technology. However, no alternatives were set up.

Finally, a teacher at a California private school wrote about their school's lack of preparedness:

No parents have inquired about opt-out yet, but we do not have a plan in place for if and when this does happen.

Case Study: An Indiana Administrator Works to Provide Opt-Out

In a rural, partly Amish district in Indiana, schools are rapidly adopting ed tech. Eric M. is the Director of Technology for the district's 2100 students. In addition to G Suite for Education, students use software from major publishers like McGraw Hill and Pearson as well as software from smaller vendors like Mobymax, Achieve3000, and Nearpod.

"It seems like every classroom you look into is using technology," Eric said. "As a technology director, that makes me both excited and scared."

Eric and his colleagues have taken several steps to protect students and support teachers—chief among them providing a strong opt-out system. Eric's district has been working on providing opt-out alternatives since before students had Chromebooks in the classroom. Eric's district serves a large Amish community, and Amish students generally decline the use of technology. In order to respect the religious and cultural views of students, the schools are well-practiced in providing hard-copy options and alternative assignments.

The district is also prepared should students abuse technology with behavior such as bullying. "Opting out is not the only reason for a student to not have a device in their hands," Eric said.

The schools provide students and their parents with a "menu" of options for opting out. In addition to FERPA-compliant options for whether or not students' names and pictures can appear in the school directory, yearbook, website, etc., families can separately choose whether or not they want their student to use technology in the classroom. This is a strong contrast to the "all or nothing" opt-out structure some schools employ, in which students who opt out of classroom technology are also automatically taken out of the yearbook.

"It's easy to do an 'all or nothing,' but I don't think it's the right thing to do," Eric said. "I wish I could take it even further than that—the ideal scenario would be to break down the use of technology a little bit more." For example, a parent might be fine with their student using all technology except for cloud services that require an account, or a parent might want their student to have access to the Internet at school but only on a family-owned device rather than a school-issued Chromebook.

Families may change their opt-out status each year. "We don't assume year after year that the same student is in the same boat," Eric said. "We find in practice that most parents aren't opting out their students, but there are a few and they have very legitimate reasons for doing so."

The difficulty of putting opt-out into practice can come from the additional burden it puts on administrators and teachers who have adopted increasingly digital pedagogical systems. As technology becomes more and more baked into lesson plans and day-to-day teaching, it can be difficult for students or teachers to function without using school-issued devices or ed tech programs. At a school issuing Chromebooks, one Iowa public school parent observed:

Most homework must be done with these laptops. I don't know how opting out would even work. Even if we used alternatives, the formats required for teachers to read assignments would make it difficult for students to submit on paper. My child's teachers all use digital submission and feedback systems, which means her data would end up there eventually even if we did opt out.

This dynamic contributed to some families' decisions not to take advantage of opt-out options even when they were available. When technology is a critical part of learning, insufficient opt-out options can mean students end up with a lower-quality or even discriminatory classroom experience. For example, one parent described refusing to let their child complete homework online, and their child receiving lower grades as a result.

Worse, some parents found that their students' participation in classroom technology continued even after they thought that had effectively opted out. A public school parent in Pennsylvania wrote:

Teachers keep creating accounts for my child on cloud apps even though I've asked the principal and teachers not to do this. They sometimes have my child use teachers' accounts.

Even when they functioned as written, opt-out policies may not have left room for parents to make specific allowances for some ed tech activities and opt out of others. Instead, this public school parent in Arizona was met with an "all-or-nothing" policy regarding Internet use in general:

The agreements are legacy agreements that were issued to get permission from parents to allow students to use wifi. They never updated the agreement, and now use it as blanket permission for anything that occurs online.

A lack of workable opt-out alternatives restricts choices for everyone, but in particular discriminates against the students who are most vulnerable to begin with: those with fewer resources who can't afford to provide their own device alternatives. For such families, the common opt-out alternative of using a personal device rather than a school-issued device is impossible. Parents as well as students felt this lack of choices. One student wrote:

I'm not a fan of data collection, but I can't afford my own computer, so I've had to compromise the past several years.

Giving parents and students the option to opt out of classroom technology use is a necessary—but not sufficient—component of protecting student privacy. In an ideal world, schools and ed tech providers would provide students with technology so beneficial and privacy-friendly that they and their parents would not even want to opt out. In reality, however, digital privacy is not a one-size-fits-all proposition, and families will always have a range of legitimate reasons for opting out of or tailoring their student's use of technology.

6. The Shortcomings of "Privacy by Policy"

Survey respondents described varying levels of trust in ed tech companies as well as schools and districts themselves. School staff generally had the most trust in "privacy by policy"—that is, the ability of policies, audits, and procedures to ensure student privacy.

A teacher in a New York private school using Chromebooks described, for example, "*an implicit trust in Google and its practices*."

A public school administrator in Indiana, however, was uncertain:

Although the service providers (Google, Microsoft, major publishers, etc.) say they are respecting student privacy, I am uncertain what is really happening in the cloud.

Parents, on the other hand, consistently were not satisfied to take the schools', ed tech companies', or states' word, and preferred to independently verify all policy claims. One public school parent in Wisconsin wrote:

The school references a special agreement between the Department of Public Instruction and our state's schools to protect student data. But I don't know what this agreement means for my child. Is data destroyed after my student leaves the district? Does Google own this data? Can they build a profile on my student? Can data be collected when teachers' correspondence or other documents discuss my child? These are all questions that should be answered. I don't feel like I should have to take the word of the school on this.

One North Carolina parent expressed a lack of confidence in state and federal law:

I have no confidence that any of my child's current or future school information will be protected by legislation.

Students showed the least trust in schools, ed tech vendors, and their policies. This lack of trust translated into increased caution and even chilling effects when students used school-issued devices and ed tech programs. One student wrote:

Because of the grey area surrounding my district's policies and general distrust of the district to uphold my privacy concerns, I am very careful about how I use my Chromebook.

Case Study: A System Administrator Advocates for Privacy Safeguards

When Matt L. started to raise the alarm about educational technology in his school district, he knew it would ruffle some feathers. As a system administrator (or sysadmin), Matt is at the center of deploying, configuring, and maintaining Google devices and software for his rural, public district's 10,000 students.

"I don't want to say that Google or Chromebooks or any of this stuff is inherently bad," Matt said. "Getting these tools into the hands of kids is hard to argue with. That's why I got into technology."

As the district has continued to expand its technology use, however, Matt has started to have concerns about consolidating students' educational and personal information in one company. "We're putting all our eggs in one basket that we're not in control of," he said. "We don't know where this student data is going."

After requests to talk about student privacy issues, Matt's boss pointed him to the district's as well as Google's privacy policies. But this did not lessen Matt's concerns.

"We have privacy policies for our website, and for our student academic records, but not so much for students' information in regards to what Google is collecting," he said. "We can't guarantee what Google is or is not doing with this information. It's all pretty vague, and it's not the kind of thing you want to be vague about."

Unsatisfied by "privacy by policy," Matt is investigating how he can implement "privacy by practice"—that is, prioritizing student privacy with active safeguards to augment and ensure existing policy, like technical settings and opt-out options.

His first step has been to "crank down the lid" on privacy settings so that students use Google products as anonymously as possible by default, without associating their online profiles with identifying information. Ideally, technical controls like these will make privacy the default in students' and teachers' work.

Matt's conversations with colleagues have moved forward in fits and starts, and are constantly changing as the district's technology situation changes. For example, a system-wide update gave Matt an opportunity to propose concurrent changes in ed tech implementation. But, soon after, discussions about abandoning local storage and migrating to Google Drive ran counter to Matt's efforts to locally control students' data. Matt remains persistent and committed to advocating for more secure, more private student systems.

"It's a really hard problem, but we need to come up with an answer," Matt said.

For many parents and students, privacy policies and even legislation were simply not enough. They wanted to know what was actually happening to students' data in *practice*, not just what was promised by policies.

7. Inadequate Technology and Privacy Training for Teachers

Survey responses showed that multiple stakeholders did not think existing technology and privacy training for teachers was keeping up with the increasing role of technology in the classroom.

Closing the skills gap for teachers is crucial because well-trained, informed staff are necessary to move beyond "privacy by policy" and implement verifiable, accountable "privacy by practice." One of the biggest problems with "privacy by policy" is that it relies on all staff members being up-to-date on complex, sometimes vague policies, and having the time and resources to comply with them consistently. Even the best policies and legislation are rendered toothless if staff members, administrators, and teachers are not equipped to implement them correctly.[17]

Parents overwhelmingly saw teachers and other school staff as unaware and non-expert in technology. Survey responses used various images here: parents described ed tech as "*the wild west*" or "*a ticking time bomb,*" and saw school staff "*jumping on the ed tech train*," working "*by the seat of their pants*," and "*winging it*."

Teachers themselves felt unequipped to handle tech in the classroom, with one describing many ed tech programs as "*too complicated for most teachers to use*." Teachers also voiced concerns about inadequate training on digital security and privacy. A public school teacher in New Mexico wrote:

No training in media literacy has been provided to teachers or students, though teachers had to watch a lame computer-generated PowerPoint to earn a certification saying we understood the ramifications of exposing school systems to outside threats or so-called "bad guys."

Another public school teacher, this one in Florida, described the lack of training and knowledge as a district-wide issue:

The county does not seem to be deliberately ignoring privacy concerns, but just lacks general knowledge about ongoing discussions about student privacy.

At the same time, teachers felt that they carried the "*burden and blame*" when privacy violations occurred in the classroom. Many observed a tension between a need for more thorough training and a lack of the funding, resources, and staffing to make that training readily available. The teachers who responded to the survey were acutely aware that, even without adequate training, they were still regarded as the first line of defense in protecting student privacy.

Case Study: An Illinois Librarian on Better Teacher Training

As a school librarian at a small K-12 district in Illinois, Angela K. is uniquely positioned to advocate for student privacy. Trained as educators, privacy specialists, and technologists, school librarians like Angela bring not only the skills but also a professional mandate to lead their communities in privacy and intellectual freedom.

In search of a balance between technology use and privacy protection, Angela is asking hard, fundamental questions about ed tech. "We can use technology to do this, but should we? Is it giving us the same results as something non-technological?" Angela asked. "We need to see the big picture. How do we take advantage of these tools while keeping information private and being aware of what we might be giving away?"

Angela wants to see more direct education around privacy concepts and expectations, and not just for students. Teachers and other staff in her district would benefit as well.

"As a librarian, I believe in the great things technology can offer," she said, "but I think we need to do a better job educating students, teachers, and administrators on privacy."

For students, Angela's district provides the digital literacy education mandated by the Illinois Internet Safety Act. However, compartmentalized curricula are not enough to transform the way students interact with technology; it has to be reinforced across subjects throughout the school year. "We used to be able to reinforce it every time library staff worked with students throughout the year," Angela said, "but now staff is too thin."

Teachers also need training to understand the risks of technology in the classroom. "For younger teachers, it's hard to be simultaneously skeptical and enthusiastic about new educational technologies," Angela said. "They are really alert to public records considerations and FERPA laws, but they also come out of education programs so heavily trained in using data to improve educational experiences."

In the absence of more thorough professional training, Angela sees teachers and administrators overwhelmed with the task of considering privacy in their teaching. "Sometimes educators default to not using any technology at all because they don't have the time or resources to teach their kids about appropriate use. Or, teachers will use it all and not think about privacy," she said. "When people don't know about their options, there can be this desperate feeling that there's nothing we can do to protect our privacy."

Angela fears that without better privacy education and awareness, students' intellectual freedom will suffer. "If students don't expect privacy, if they accept that a company or a teacher or 'big brother' is always watching, then they won't be creative anymore," she said.

8. Opportunities for Digital Literacy Education for Students

Most students who responded to the survey were unsure of what ed tech meant for them and why they should care. Just as staff need training to implement ed tech services with digital privacy in mind, students need enhanced education to safely use such services.

One California public school student wrote:

I am confused about the specifics of what my technology rights are as a student. Technology is confusing, and I know little about how my data is stored and how that affects me.

One public school student in New Mexico specifically voiced a desire for courses on technology:

I feel like in order to start using these devices, we should be taking courses to understand them first.

On the other end of the spectrum, student respondents who were acutely aware of privacy issues were most concerned that their peers were unaware of—or worse, apathetic about—the threats ed tech posed to their digital privacy. One particularly tech-savvy student wrote,

What I'm worried about most in this school is apathy related to privacy. It seems a lot of students don't care about privacy issues whatsoever.

Students' digital literacy education will be crucial to any long-term plan to put students and their families—not ed tech companies or vendors—back in control of students' private information. Rather than being at odds with each other, ed tech and digital literacy can and should work hand in hand, with technology use in the classroom supporting students' growing awareness of the Internet, their online data trails, privacy expectations, and common-sense measures for protecting their privacy in an increasingly digital world.

Part 2: Legal Analysis

The regulatory regime protecting students' privacy in the United States is a complex patchwork of federal and state statutes as well as voluntary industry self-regulation. Unfortunately, despite the abundance of laws nominally protecting student privacy, companies' actual privacy practices leave much to be desired, and state and federal legislation has not been able to keep up with ed tech's rapid growth.

After discussing industry self-regulation and the Student Privacy Pledge, we provide an

analysis of key federal laws FERPA and COPPA followed by a sample of outstanding state laws in California, Colorado, and Connecticut.

Industry Self-Regulation

Loopholes in the Student Privacy Pledge

Developed by the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) in the fall of 2014, the Student Privacy Pledge is intended, in its own words, "to safeguard student privacy regarding the collection, maintenance, and use of student personal information."[18] While it's not a law, the Student Privacy Pledge is indeed designed to be legally enforceable by the Federal Trade Commission (FTC), which may bring enforcement actions against companies that make but then break public promises. This means its over 300 signatories[19] have made what appears to be an essentially binding commitment to its 12 provisions.

In many cases, however, the Pledge's loopholes prevent it from offering meaningful protection to student data. The problems with the Student Privacy Pledge are not in its 12 large, bold commitment statements, but in the fine-print definitions under them.[20]

First, the Pledge's definition of "student personal information" calls into question the basic integrity of the Pledge. By limiting the definition to data to that is "both collected and maintained on an individual level" and "linked to personally identifiable information," the Pledge seems to permit signatories to collect sensitive and potentially identifying data such as search history as long as it is not tied to a student's name. The key problem here is that the term "personally identifiable information" is not defined, allowing companies to collect and use a significant amount of data outside the strictures of the Pledge. This pool of data potentially available to ed tech providers is more revealing than traditional academic records, and can paint a picture of students' activities and habits that was not available before.

By contrast, the federal definition of "personally identifiable information," found in FERPA and its accompanying regulations,[21] is broad and includes both "direct" and "indirect" identifiers, and any behavioral "metadata" tied to those identifiers. The federal definition also includes "other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." While the Pledge presumably was not intended to run counter to federal law, FERPA applies only to schools that receive federal funding, not to all schools across the country.[22]

Second, the Pledge's definition of "school service provider" is limited to providers of applications, online services, or websites that are "designed and marketed" for educational purposes.

A provider of a product that is marketed for and deployed in classrooms but was not necessarily "designed" for educational purposes is outside the Pledge. The Pledge also excludes providers while they're providing "general audience" apps, online services, and websites. We alleged in our FTC complaint against Google that the Pledge does apply to data collection on "general audience" websites when that data collection is only possible by *virtue of a student using log-in credentials that were generated for educational purposes*. However, SIIA, a principal developer of the Pledge, argued to the contrary and said that the Pledge permits providers to collect data on students on general audience websites even if students are using their school accounts.[23]

The Pledge's definition also does not include providers of devices like laptops and tablets, who are free to collect and use student data contrary to the Pledge.

Simple changes to the definitions of "student personal information" and "school service provider"—to bring them in line with how we generally understand those plain-English terms—would amount to more meaningful protection of student data.

Potential Violations of the Pledge

The first item in the Pledge is a promise to refrain from collecting, using, or sharing students' personal information except when needed for legitimate educational purposes or if parents provide permission:

> Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.

After an extensive investigation, we found that Google's educational software platform G Suite for Education falls far short of the Student Privacy Pledge, to which Google is a signatory. Despite publicly promising not to, Google mines students' browsing data and other information[24] and uses it for the company's own purposes. Making such a promise and failing to uphold it is, in EFF's view, a violation of FTC rules against unfair and deceptive business practices.

In December 2015, we filed an FTC complaint urging the Commission to investigate Google's failure to live up to its commitments under the Pledge. Unfortunately, the FTC has taken no action that we are aware of to date.

Federal Law

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a federal law that applies to districts and schools that receive federal funding. It forbids schools from disclosing student information without parental consent, but it has limitations: it only applies to certain types of student information and there are exceptions that can be exploited. The law is enforced by the U.S. Department of Education, which can cut off funding to noncompliant schools.

FERPA protects students' "education records"[25] including personally identifiable information.[26] The law also protects information about students' online activity when they are using school-issued devices, when that information is tied to personally identifiable information; according to the U.S. Department of Education, FERPA protects behavioral "metadata" unless it has been "stripped of all direct and indirect identifiers."[27]

FERPA generally prohibits school districts from sharing student information with third parties without written parental consent. Sometimes school districts use a loophole in the law to get around the parental consent requirement by characterizing ed tech companies as "school officials." However, the school official exception[28] is only applicable to a contracting company if specific conditions are met:

- The school district may only share student information without written parental consent with a contractor who has been determined to serve legitimate educational interests. A school district must articulate specific criteria in its annual notification of FERPA rights and a contractor must meet those criteria.
- A contractor may receive student information without written parental consent if the company is under the direct control of the school district with respect to the use and maintenance of education records. Usually this requires very specific contract terms between the district and the company.
- A contractor cannot use student information for any other purpose than the purpose for which it was disclosed by the school district. Again, this usually requires very specific contract terms that limit what data the contractor may collect from students and how it may use that data. The contract should also clarify the interaction between its terms and the company's general Terms of Service and Privacy Policy.
- The contractor must perform an institutional service or function for which the school district would otherwise use employees.

The ease with which ed tech providers can take advantage of the school official exception described above prevents FERPA from going far enough to protect student data.

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) is a federal law that applies to online companies and is enforced by the Federal Trade Commission.

COPPA requires companies to obtain "verifiable parental consent"[29] before collecting personal information from children under 13 for commercial purposes. Personal information can include traditional personally identifiable information such as a child's name or contact information as well as online behavioral data—that is, what a child does online.

A key question in the education context is whether a school district can provide consent to collect student data to a company on behalf of the parents, or whether the company must get consent directly from the parents.

The FTC made clear that if "an operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent."[30]

Specifically, a school district should ask: "Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service?" If the answer to these questions is "yes," the district "cannot consent on behalf of the parent."

State Law

Student privacy has been a priority in state legislatures in recent years, with 49 states and the District of Columbia introducing 410 bills addressing student privacy since 2013. Of those, 36 states have passed 73 student privacy bills into law.[31] Building on comprehensive surveys of state student privacy law,[32] here we highlight three states that stand out: California, Colorado, and Connecticut. First we analyze California's student privacy law, the first state to attempt to regulate ed tech companies. Next we discuss Colorado and Connecticut, both of which took the new step of distinguishing between third parties with which schools do and do not have contracts.

California – Student Online Personal Information Protection Act (SOPIPA)

Passed in 2014 and effective starting in 2016, California's Student Online Personal Information Protection Act (SOPIPA)[33] aims to improve privacy and security for student educational records. SOPIPA was the first attempt to regulate ed tech companies, and several other states have passed student privacy acts that track and expand on SOPIPA in their own states.

SOPIPA protects not only traditional personally identifiable information such as name, birthdate and student ID number, but also online behavioral data such as "search activity." It may be enforced by the California Attorney General (and possibly also private citizens if they can show monetary loss) under Business & Professions Code § 17200.

The law prohibits a company from engaging in targeted advertising on its own website or any other website "when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that the operator has acquired" from a student's use of the website. A service provider also may not "use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a K–12 student except in furtherance of K–12 school purposes." Data collected on students also may not be sold.

In short, ed tech companies cannot create student profiles or target students for non-educational purposes.

SOPIPA provides important privacy protections for K-12 students, but it also includes significant loopholes. SOPIPA expressly "does not apply to general audience Internet Web sites, general audience online services, general audience online applications, or general audience mobile applications, *even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications*."

Thus, SOPIPA prohibits a company like Google from serving targeted ads within G Suite for Education and through its DoubleClick ad network on third-party websites *based on* student behavioral data obtained from the use of G Suite. But when students are logged into their Google account and navigate outside of the education apps, SOPIPA permits the company to collect student behavioral data for a variety of purposes, including serving ads.

SOPIPA may also allow a company to collect a broad array of browser data when students are logged into a device (e.g., a Chromebook). The law defines "operator" as an operator of "an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes." It is not clear if a device or browser fits into this definition.

SOPIPA also leaves questions open regarding data retention. While websites and other services are directed to delete students' information if requested by the school or district, SOPIPA does not state a time period in which website and service providers must comply, nor does it include any other requirements for data retention and deletion.

While SOPIPA leaves large loopholes open and questions unanswered, it also paved the way for other states to build on it in their own student privacy legislation.

Colorado – Student Data Transparency and Security Act (SDTSA)

In 2016, Colorado passed the Student Data Transparency and Security Act (SDTSA)[34] to improve protections for student personally identifiable information (PII). Building on California's SOPIPA, the SDTSA delineates obligations for the state Department of Education, district and charter schools, and service providers.

The SDTSA covers student PII, which it defines as "information that, alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a school service, or by a school service contract provider or school service on-demand provider."

Like SOPIPA, SDTSA prohibits targeted advertising to, or creating a non-educational profile of, a student based on information gleaned over time from the student's online behavior, use of educational applications, or student PII.

In a step that goes beyond SOPIPA, Colorado's law recognizes and creates obligations for two different types of service providers: "school service contract providers," or entities that enter into formal, negotiated contracts with public educational entities to provide a school service; and "school service on-demand providers," or entities that occasionally provide school services to a public educational entity, or to a school's employees, under standard, non-negotiable terms and conditions. When schools do enter a contract with third-party service providers, the law requires clauses specifying that student data is to be deleted when no longer needed for purposes of the contract, limiting the use of student information to noncommercial purposes specified in the contract, and specifying penalties for noncompliance.

SDTSA also takes steps to improve transparency by requiring that the state board of education and local schools publish on their websites the type of data points collected by third-party service providers, including why each data point is collected, how it is used, and why it is shared. This makes important privacy-related information more easily accessible to students, their parents, and any other concerned parties.

Further, the law requires that all district and charter schools adopt a student privacy and data protection policy. To help schools that have less local capacity, the state Department of Education must provide them with a sample policy, including protocols for maintenance of a student data index, retention and destruction of student personally identifiable information, use of student personally identifiable information, prevention of security breaches, requirements for contracting with service providers, and disclosure

of PII. These privacy policies must be made available to parents and students and posted on schools' websites.

Finally, the SDTSA is unique in its explicit focus on training local staff to handle student data. The law requires the state's Department of Education to identify training resources and make them available to school districts, a crucial step toward ensuring long-term protection for student privacy.

Connecticut – An Act Concerning Student Privacy

In 2016, Connecticut enacted "An Act Concerning Student Privacy."[35] Like California's SOPIPA and Colorado's SDTSA, this law prohibits service providers from using student information for targeted advertising of students.

The law defines "student information" as "personally identifiable information or material of a student in any media or format that is not publicly available" and is provided by a student (or her parent or legal guardian) to the service provider, created by an employee or agent of a school for school purposes, or gathered through the service provider's platform and capable of identifying the student. The law contains a nonexclusive list of data points that qualify as student information, including email addresses, disciplinary records, test results, health records, biometric information, food purchases, and text messages.

Similar to Colorado's provisions for training resources, Connecticut's law establishes a task force to study student privacy issues, including investigating the creation of a toolkit for local and regional boards of education to improve data contracting practices, increasing employee awareness of student data security best practices, developing a list of approved softwares and websites, and increasing transparency on privacy information for parents.

The law also sets out requirements for school contracts with service providers. Any time a local or regional board of education plans to share student data with a service provider, the board must enter into a written contract with the service provider. The law contains a nonexclusive list of terms that the contract must contain, including a statement that student information does not belong to the service provider, a description of means through which the board may request deletion of student information, and a statement that the service provider will ensure the security and confidentiality of student information.

These contract provisions extend to ensuring parents are notified promptly. Each time a contract is executed with a contractor, the regional school board must notify any student affected by the contract, as well as their parents, within five business days. The notice must include a description of the contract (including what student information may be collected under it) and must be posted on the board's website.

Conclusion

At both the state and federal level, tighter legislation is needed to close loopholes and give school districts the structure and resources necessary to provide transparency and choice to students and their families. Industry self-regulation like the Student Privacy Pledge does not go far enough to remedy such loopholes. The ed tech industry has moved faster than legislation aimed at protecting student privacy.

Part 3: Recommendations

Ensuring student privacy requires participation from a number of stakeholders. Below, we outline specific recommendations and best practices. After making recommendations for school policies and communications, we turn our attention to various school stakeholders, including administrators, teachers, librarians, system administrators, parents, and students. We conclude with best practices for ed tech companies.

Recommendations for School Procedures

This section draws on common pitfalls EFF has seen in parental disclosure forms, Acceptable Use Policies (AUPs), opt-out practices, and other procedures that shape what students and parents know about ed tech in their school or district, and what choices they are able to make based on that information.

While EFF's focus has been on ed tech companies' policies and practices rather than those of schools, it is important to highlight that school privacy policies and their implications change once ed tech is in the picture. For students and parents on the ground in particular, the distinction between the privacy practices of large ed tech companies and the privacy practices of one's own school or district is not always clear. With this in mind, we offer suggestions for better, more privacy-conscious school policies and communication.

- Parents should be given adequate time to review and consider all materials.
- The school or district should ensure that its AUP is separate from the privacy policies and other materials pertaining to individual ed tech providers. It should be clear to the parents and students which entity each document pertains to.
- The AUPs should not be overbroad, and should be limited to the new technology being implemented. The school or district should not use it as an opportunity to police student conduct outside of the educational context (e.g., clauses that dictate what students can and cannot say on social media) or to grant itself additional authorization (e.g., giving school officials the right to conduct searches of students' devices).
- In no circumstances should AUPs be used to waive students' (or their parents') statutory or constitutional rights.

- Does the AUP say the extent to which it allows the school or district to monitor students' use of the educational technology? And if so, is it narrowly tailored to the educational context?
- Consider carefully how the school or district's AUP connects with the privacy practices of the ed tech provider. For instance, does it say that the district reserves the right to renegotiate the privacy terms with the vendor? Can the district authorize the vendor to release student data?
- To the extent possible, schools should prepare contingency plans—opt-out policies and/or alternative technologies—if parents and/or students find the data practices of a particular vendor concerning.
- Schools and districts should avoid asserting authority to consent on behalf of parents to the sharing of student data with third parties such as ed tech vendors, and should obtain written consent from parents directly.

Recommendations for School Stakeholders

School Administrators

School administrators are under pressure to employ technology to improve student performance. But when at the negotiating table with ed tech vendors, administrators must balance that pressure with their responsibility to protect the privacy of their students. The following recommendations draw on our own interactions with school administrators as well as the federal Department of Education's guidance for administrators.[36]

Don't accept Terms of Service when you can get a contract. The vendor should be willing to customize contract terms to address a particular school or district's privacy concerns. Enter into a written contract or legal agreement with service providers when possible. These contracts should include provisions on security, collection, use, retention, disclosure, destruction, access, and modification of data.

Critically review the terms of "click-wrap" license agreements on consumer applications. When schools and districts can't negotiate agreements and are consequently required to accept a provider's Terms of Service in order to use the application, they must cautiously review the Terms of Service. Because the Terms of Service may change without notice, schools and districts should regularly re-read the terms to be aware of any relevant changes. The Department of Education has published a useful resource that offers specific guidance for schools and administrators as they evaluate potential Terms of Service agreements from service providers. [37]

Build local capacity to evaluate ed tech services. There is no substitute for building capacity within a school or district to conduct an independent review of third-party providers' practices and policies as they pertain to privacy. Do not rely on outside sources alone—like the Student Privacy Pledge or other evaluations—when determining which

vendor to work with. Instead, draw from multiple resources as well as an independent evaluation when choosing ed tech services. Develop school and district-wide policies and procedures to evaluate proposed online service providers. District and school leadership, as well as teachers, should be aware of how services can be approved and who has the authority to enter into agreements with providers. This evaluation process should take into consideration privacy and security concerns relating to the services.

Get familiar with the school or district's ed tech ecosystem. As new services are adopted, maintain a publicly accessible list of all the vendors that the school or district partners with, along with the corresponding privacy policies and any school or district evaluation.[38] Ensure that staff do not use services beyond the ones the district has negotiated with and/or evaluated and approved—and, when they do, get it evaluated and publicly listed as soon as possible.

Ask the right questions. Examine potential ed tech partners with a critical eye. In addition to thinking about pedagogy and learning benefits, ask questions about data collection, privacy, and transparency. Some questions to think about include:

- What data will the vendor collect? Data should not automatically be collected for purposes beyond student education—for instance, product improvement. If data must be used for product improvement or other non-educational purposes, it should be properly anonymized and aggregated.
- Does the vendor follow current best practices in data security?
- Does the vendor give advance notice when it changes its data practices?
- Will the vendor disclose any student data to its partners or other third parties in the normal course of business? If so, are those conditions clearly stated? What are the privacy practices of those other entities?
- In a hardware product like a laptop, are controls available to prevent the vendor *and* school district employees from using the devices' webcams, microphones, and location-tracking features to spy on students?

Notify parents. Be transparent with parents and students regarding how the school or district—and third-party vendors and companies—collect, share, protect, and use student data. The school or district should not sign students up for any service without getting explicit permission from their parents. Parents should have access to all relevant privacy policies of vendors and ample time to consider whether they feel comfortable with the proposed vendors' data practices.

Provide choices. Provide meaningful opt-out processes that give parents and students control over their use of technology in the classroom. Make opt-out processes "granular," with separate options for different uses of student data, e.g., putting information in the yearbook/directory, using cloud services, using school-issued devices vs. personal devices, using services that do or do not have a contract with the school, etc. Prepare teachers and

other staff to provide educationally comparable alternative assignments and activities for students who choose to opt out.

Teachers

Teachers play the role of intermediaries between students and the technology being deployed in classrooms. In addition to administering technology directly to students, teachers can integrate digital literacy and privacy education across their existing curricula.

Make digital literacy part of the curriculum. Ensure that students are learning basic digital privacy and security techniques while utilizing new ed tech tools, including creating strong passphrases for their online accounts.[39] Additionally, when applicable, convey that the data the students submit as part of their educational activity (including, for example, search terms, browsing history, etc.) will be sent to another entity and they should therefore exercise caution in sharing sensitive personal information.

Advocate for better training for teachers. Teachers' own digital literacy and privacy training is often overlooked when new ed tech services are introduced to the classroom. The best way to sharpen your expertise and protect your students is to enhance your own professional privacy knowledge. Advocate for training within the school/district or seek out support from external resources.

Get parental consent. Refrain from signing students up for services without getting explicit written consent from parents.

Pick ed tech tools carefully. Exercise caution when choosing what devices, platforms, services, or websites to use in the classroom. When tools are available for free on the web, for example, it can be tempting to adopt and use them in an ad hoc manner. However, each tool may pose different risks to students' personal data. Instead, go through your school or district's approval process, or seek additional opinions, before adopting new ed tech tools.

Find allies. If you are concerned about a particular technology and its privacy implications, find allies amongst your colleagues**.** Seek out other staff who share your concerns and coordinate with them to better advocate for student privacy across your school or district.

Librarians

With professional training and ethical commitments that prioritize user privacy, school librarians are in a unique position to advocate for student privacy. In addition to the recommendations below, refer to the American Library Association's (ALA) privacy checklist for school libraries.[40]

Lead by example with the library's privacy policy. Refer to the ALA's guidelines for school library privacy policies[41] to protect students' privacy when they interact with the library's systems, applications, and collections. Limit personal information collection and retention to the bare minimum required to provide services, and ensure that it is stored in an encrypted form. Critically, the library privacy policy should also detail when student library records can be shared and with whom.

Go above and beyond privacy law. School librarians' duty to protect student information sometimes goes beyond FERPA requirements.[42] For example, FERPA may permit disclosure of student library records to parents or school officials where state library confidentiality statutes and professional ethics otherwise prohibit it. FERPA, however, does *not* require schools to create or retain any such records. Concerned librarians can tailor their data collection and retention policies to protect students' confidentiality and reading freedoms with this in mind.

Conduct privacy audits, both within the library and in the school's or district's larger ed tech ecosystem. Whether ed tech services are adopted top-down by large contracts with the administration or bottom-up by individual teachers in single classrooms, librarians can be a central resource for investigating their privacy risks. In addition to getting involved with large-scale contract negotiations, think about how to ensure the quality and safety of websites, apps, and services adopted on a more ad hoc basis by teachers. Survey staff to get an idea of who is using what services, and periodically review them. Do their privacy policies or agreements with the school address collection, use, aggregation, retention, and encryption of students' PII? Do third-party services respect school policies? Are they in compliance with applicable state law?

Get a seat at the negotiating table. Advocate for student privacy at every stage, but especially before new software and devices are adopted. Librarians have the training and experience to approach vendor relations and contract decisions with student privacy in mind. When your district negotiates contracts with a new ed tech vendor, find out how to be involved in the process.

Educate staff, colleagues, teachers, and decision makers about student privacy. Initiate conversations about student privacy with colleagues at all levels. The school or district might create policies and processes that threaten student privacy. This presents an opportunity to educate decision makers about the value of student privacy and the danger of violating it, as well as about how to better craft policy in the future.

Take the lead in making digital literacy and privacy rights a key part of students' curricula. As both educators and privacy experts, librarians play a unique role in students' digital literacy education. In the library, incorporate lessons and resources about students' privacy rights and protecting themselves online. Book discussions, movie nights, and displays can be effective; see the ALA's Choose Privacy website[43] for additional

resources and ideas. In addition to teaching within the library, share resources with teachers to encourage reinforcing digital privacy lessons across classes and curricula.

System Administrators

System administrators (or sysadmins) are at the center of ed tech implementation, and can take the first crucial steps in protecting students' privacy at scale. They are in a particularly good position to implement "privacy by practice" with technological safeguards on top of any existing "privacy by policy" from school and ed tech company policies.

Lock down privacy settings. Do not trust defaults. Take advantage of available settings and options in students' devices and software to make sure they are as privacy-hardened as possible. For schools using Google services, you can start by referring to our guides on Google accounts[44] and Chromebooks.[45] Keep in mind that products and user-interfaces are updated often, so you may need to review options regularly to ensure they are set at their most privacy-protective.

Generate and administer strong logins and passwords. One common pitfall to avoid in ed tech implementation is weak logins and passwords. Generally, such weak credentials include personally identifiable information (such as student ID, first and last name, date of birth, etc.), are short or not complex enough to be considered strong passwords, or both. Take control of password generation and administration to make sure students have strong, randomly generated passwords. Even better, educate students in strong password management and require them to create a new password when they first log in.

Be a resource for selecting ed tech tools. In addition to being responsible for administering, configuring, and maintaining a school or district's ed tech tools, sysadmins can function as in-house experts in selecting the right ed tech tool for a given problem or purpose. Take notice of discussions about services with which to contract as well as teachers' ad-hoc adoption of tools for single-classroom use.

Find allies. If you are concerned about a particular technology and its privacy implications, find allies amongst your colleagues**.** Seek out other staff who share your concerns and coordinate with them to better advocate for student privacy across your school or district.

Parents

Based on the inquiries we receive regularly at EFF, it is clear that parents across the country are concerned about the privacy implications of technology in the classroom. Parents are in a strong position to advocate to schools and districts on behalf of their children.

Ask the right questions. As a parent, be on the lookout for:

- What kind of devices, applications, and other technology are being used to teach your child?
- Were you presented with the opportunity to review the privacy policies of these vendors?
- What data are the technology providers and the school district collecting, respectively? Do vendors and schools clearly communicate why they're collecting that data?
- Are the technology vendors using current best practices to protect the data collected on your child?
- You should be able to choose whether or not any use of your child's data is collected or used for purposes beyond student education—for instance, product improvement. If data will be used for product improvement, is it properly anonymized and aggregated?
- Will the vendor disclose any student data to its partners or other third parties in the normal course of business? If so, are those conditions clearly stated? What are the privacy practices of those entities?
- In a hardware product like a laptop, are controls available to prevent the vendor *and* school district employees from using the devices' webcams, microphones, and location-tracking features to spy on students? What are the school or district's policies on using those features?

Push for opt-out alternatives. Outline your privacy concerns to the school or district and ask for options to opt out of technology use, or to use different devices or software. If opt-out processes are not in place, advocate for their creation. People to reach out to might include your children's teachers, technology directors, principals, and parent-teacher association leadership.

Find allies. You can find allies both locally within your school or district as well as elsewhere through national networks of other concerned parents. Some tips for connecting with parents locally include:

- Raise your concerns with parents you already know well. Do not try to convince anyone—just look for two or three others who already share your concerns.
- If you cannot easily find at least two other parents who share your concerns, approach your child's teacher(s) and ask whether they know any other parents who might share your concerns. Ask your child if any of his/her peers and classmates have raised concerns and speak with their parents.
- Hold a discussion group for a small group of parents. Discuss what information other parents have received from the school or district, and which other parents share your concerns and want to work together.

Once you have identified a small group of parents to work with:

- Attend a Parent Teacher Association (PTA) or equivalent meeting together and raise your concerns. Make sure everyone in your groups speaks and collect contact information of other similarly-minded parents who may be potential allies.

- Contact your district and/or school administrators and request a meeting with all the parents in your group. Make sure everyone in your group speaks. Ask district or school officials to explain the process through which the current technology and policy was adopted, and how it might be changed. Ask district or school officials to provide training to teachers, administrators, and students about best practices for protecting student privacy and digital literacy generally. Lastly, see if the district or school officials can propose other solutions to your concerns.
- Contact a member of your school board and request a meeting with all the parents in your group. Make sure everyone in your group speaks and ask the school board member whether they would consider sponsoring a measure constraining school or district contracts to prevent intrusive data collection.

Students

Given that the integration of technology in education affects their data personally, it's vital that students are especially attentive to what's being integrated into their curriculum. Below, we provide a few recommendations for students to act to preserve their personal data privacy:

- Determine if there are privacy settings you can control directly in the device or application.
- Try to ascertain the privacy practices of the ed tech providers your school uses.
- Avoid sharing sensitive personal information (which could include, for example, search terms and browser history) if it will be transmitted back to the provider.
- If you're concerned by the usage of a certain service and find it intrusive, talk to your parents and explain why you find it concerning.
- Ask to opt out or use an alternative technology when you do not feel comfortable with the policies of certain vendors.
- Share your privacy concerns with school administrators. It may work best to gather a few like-minded students and have a joint meeting where everyone shares their concerns and asks the school administrator(s) for further guidance.

Best Practices for Ed Tech Companies

Finally, we provide best practices for ed tech companies, both for providing ed tech services in a privacy-conscious manner and for respecting student privacy on other, non-educational services.

Of particular concern to EFF is the way that some of the largest Internet companies treat students' data when students use their non-educational services. For example, as the largest provider of cloud-based educational software, Google necessarily has access to a broad array of students' online behavior: within Google's education apps, on other Google properties, and on third-party websites that use Google's ad services. Unfortunately, despite seeming to promise not to track students, the only categorical

commitment Google makes is to only refrain from displaying targeted ads to students on Google properties.[46]

Providers can implement the recommendations below while realizing their mission to improve student academic performance. Here we draw on our own interactions with ed tech stakeholders as well as the California Attorney General's ed tech guidelines.[47]

Data collection. Collect data only to the extent that it's necessary for educational purposes. Get written opt-in consent from parents—or, at the bare minimum, offer opt-out—if you intend to collect data for product improvement. If data must be collected for product improvement, aggregate and anonymize it. Do not track students' online behavior to create a profile on them, even when they navigate away from core educational services. Finally, set default settings on devices and software to protect against, rather than allow for, privacy-invasive data collection.

The U.S. Department of Education has published guidance for service providers to use "learning analytics" techniques to improve ed tech products.[48] However, the guide ignores the privacy implications of using data analytics and readily acknowledges that a full discussion of privacy is "beyond the scope of the document." Essentially, the guide assumes that data collection is a foregone conclusion, and doesn't begin to address the question of whether data *should* be collected in the first place, how to weigh the benefits and risks, how to get consent before collecting data, or how to manage the data once it's been collected. As a result, service providers should exercise extreme caution before following the suggestions in the Department of Education's guide.

Data use. Describe the different purposes for which various types of student data will be used. No student data, including covered information and persistent unique identifiers, should be used to engage in targeted advertising or to create profiles of students.

Encryption. Ensure that all student data is at least encrypted in transit, and employ current best practices to implement HTTPS, encrypt data at rest, and secure student accounts.

Data retention. Data should only be retained for the duration that a student uses the service, or for a duration specified by the school or district, and then promptly deleted.

Sharing and third parties. When disclosing information to other service providers and third parties, verify their privacy policies and practices. In particular, ensure that third parties do not further disclose student information. When disclosing information to researchers in particular, confirm that the disclosure is permissible under federal and state law or that the disclosure is directed by a school, district, or state education department.

Finally, describe in your privacy policy all third parties with which student information is shared, what information is shared, and the purpose of sharing it. Whenever possible, obtain explicit written consent from parents before sharing. If a service links or in any way directs students to other websites or service providers, also disclose these referrals in your privacy policy.

Working with districts. Actively discourage schools and districts from bad password hygiene—for instance, using students' birthdays and last names as passwords. Go further to implement safeguards to prevent weak passwords (e.g., do not allow passwords that consist of only 6-8 numbers.) Engage with school staff and system administrators to educate them on privacy safeguards and privacy-conscious uses of a given ed tech service.

Transparency. Make privacy policies as detailed and understandable as possible. The policies should be conspicuous, readable (in plain language), available in a single location, and not embedded in Terms of Service or Terms and Conditions statements. Include at least the following points:

- A description of what student information (PII, behavioral data, etc.) is covered, as well as the extent to which the PII of other users (e.g., parents, guardians, and educators) is covered.
- A comprehensive description of the types of data collected, the methods of data collection, and data minimization measures used to collect only necessary information, or as directed by the school or district.
- A comprehensive description of how data is used, avoiding meaningless statements such as "to improve products and services."
- How long data is retained and why. Further, develop a system to respond to requests from schools or districts for deletion of student data.
- Any third-parties that may have access to student data and under what circumstances and for what purposes.

The policies should contain a privacy contact for users to get in touch with providers regarding privacy practices.

In addition to privacy policies, include privacy-related information as part of user interfaces when appropriate. Make related materials accessible in a "one-stop shop" for various stakeholders—parents, teachers, administrators, and students—to review all terms of service, privacy policies, and other digital privacy-related information.

Conclusion

While schools are eagerly embracing digital devices and services in the classroom—and ed tech vendors are racing to meet the demand—student privacy is not receiving the attention it deserves.

Together, our survey testimony and legal analysis offer a user-focused approach to defining the problems and risks around student privacy, particularly lack of transparency, lack of choice, and a technical landscape that has outpaced legal safeguards. As our recommendations outline, parents, students, and school staff can take effective action to advocate for and raise awareness about student privacy.

Ultimately, however, meaningful improvements in student data protection will require changes in state and federal law, in school and district priorities, and in ed tech company policies and practices.

Appendix

Survey Questions

1. Which best describes you? (Select one.)
    - I'm a parent reporting on my child's school practices.
    - I'm a student.
    - I'm a teacher reporting the practices at the school where I teach.
    - I'm a district/school administrator reporting what happens in my district/school.
    - I'm a concerned individual.

2. Are you over the age of 13?
    - Yes.
    - No. *[If no, survey ended and user redirected.]*

3. Name of district or school

4. Location of the district or school you are reporting

5. State

6. Does the district/school issue any of the following devices? (Select all that apply.)
    - Google Chromebook
    - Other type of laptop
    - iPad
    - Microsoft Surface
    - Other type of tablet
    - Other

6a. *[If "Other"]* What other devices were issued by your district/school?

7. The district/school… (Select all that apply.)
    - Issued a specific device to each student, and students can take their device home.
    - Issued a specific device to each student, and it stays at school.
    - Provides devices for the classroom in a communal pool of devices that any student can use.
    - Other

7a. *[If "Other"]* Please explain.

8. Students affected by the practice (Select all that you can confirm apply to your district/school.)
    - Kindergarten

- 1st grade
- 2nd grade
- 3rd grade
- 4th grade
- 5th grade
- 6th grade
- 7th grade
- 8th grade
- 9th grade
- 10th grade
- 11th grade
- 12th grade

9. Which of the following is the direct/schoool using?
- Google Apps for Education (GAFE)
- Microsoft in Education
- Other cloud-based services
- Other applications

9a. *[If "Other applications"]* What other applications is the district/school using?

10. Are parents provided with written disclosures about data collection (such as a privacy policy)?
- Yes, from the school alone.
- Yes, from the company providing services.
- Yes, from both the school and the company.
- No.
- I don't know.

11. Can parents opt their children out of participation in the technology?
- Yes, and the school/district provided an alternative technology option.
- Yes, but the school/district did not provide an alternative technology option.
- No.
- I don't know.

12. How concerned are you about the privacy implications of school-issued devices?
- Not concerned at all
- Neutral
- Concerned
- Extremely concerned

13. Additional information you'd like to share with us

Apps, Software, and Services Reported in Survey

In response to question 9a in the survey above ("What other applications is the school/district using?"), survey respondents reported the following apps, software, and services as in use in the classrooms in their school or district.

ABCYa!
Absolute Safe Schools Program
Achieve 3000
Accelerated Reader 360
Agile Mind
ALEKS
Animal Jam
Apex Learning
AraLinks
Ascend
Audacity
Barracuda
Big Ideas Math
Blackboard
Bloomz
Blucoat Filtering
Book Creator
Bright Bytes
Brain Pop Jr.
CAPE
CaSecureBrowser
Canvas
Casper Suite
CERAN
Class Dojo
Clever
Code.org
Compass
Connexus
Dimension U
Discovery Education
Doceri Interactive Whiteboard
Dream Box
Dropbox
eBackpack
eCampus
Echo

Edmodo
Edline
Edsby
Edureactions Interactive Whiteboard
Encore
Engrade
enVision Math 2.0
eSchool Data
Evernote
Explain Everything
Fee Pay
FlipGrid
Geometers Sketchpad
Global Protect
Gmetrix
GoMathDaily
Grade Connect
GUS Communication App
Haiku
Illuminate
Info Snap
iMovie
iReady
iSafe Digital Learning/iSafe Digital Programming
iStation
Infinite Campus
Itslearning
iXL
Go Guardian
GraphingCalc
Hapara
Hoodamath
Instagram
Jamfnation
Kahoot
LanSchool
LaunchPad
Lexia
LiveBinders
Logger Pro
Lucid Chat
Meraki
MindMup
Minecraft Edu

MiStar
Magister
Merriam-Webster Dictionary app
Mobymax
Moodle
MyBigCampus
Myhomework
myON
Naviance
Nearpod
Netop
NoRedInk
Notability
Padlet
PearDeck
Pearson Success
PeachJar
Popplet
PowerSchool
Prezi
Prodigy
Propel Mobile School
QuikSchools
Quizlet
RapidIdentity
Raz-Kids
ReadyGen
Remind.com
Rosetta Stone
Sakai
Samarbeta.net
Scholastic Reader
Skills Tutor
SchoolLoop
Schoology
Scoop.it
SecURLy
See Saw
Showbie
Skyward
Smarter Balanced Assessment
SapTrends
Socrative
SpeakIt

Spelling City
ST Math
Storyboard That
Story Jumper
Study Island
Subtext
Sumdog
Super Kids Reading
SynchronEyes (SMART Technology)
Tackk
TeacherEase
Teachscape
Tellagami
TenMarks
Thinglink
TI Inspire CAS
Ticket to Read
Toontastic
TurnItIn
Type2Learn
Typing.com
Typing Pals
Twitter
Weebly
Wixie
Xtra Math
YouTube

1 David Nagel. (Apr. 8, 2014). One-Third of U.S. Students Use School-Issued Devices. *The Journal*. https://thejournal.com/articles/2014/04/08/a-third-of-secondary-students-use-school-issued-mobile-devices.aspx

2 Harriet Taylor. (Dec. 9 2015). Google's Chromebooks make up half of U.S. devices sold. *CNBC*. http://www.cnbc.com/2015/12/03/googles-chromebooks-make-up-half-of-us-classroom-devices.html

3 Bram Bout. (Apr 30, 2014). Protecting Students With Google Apps for Education. *Google Cloud Official Blog*. https://cloud.googleblog.com/2014/04/protecting-students-with-google-apps.html

4 Anthony E. Kelly and Mike Seppala. (2016). Changing Policies Concerning Student Privacy and Ethics in Online Education. *International Journal of Education Technology*, 6(8), 652-655.

5 See https://www.eff.org/issues/privacy/.

6 See https://ssd.eff.org/.

7 Billings, K. (2015, February 24). SIIA estimates $8.38 billion US market for preK-12 educational software and digital content. *SIIA Blog*. http://www.siia.net/blog/index/Post/62376

8 Ferreira, J. (2012, November 3). Knewton - Education datapalooza. https://www.youtube.com/watch?v= Lr7Z7ysDluQ

9 U.S. Department of Education, Office of Educational Technology. (2013). Expanding evidence approaches for learning in a digital world. http://tech.ed.gov/wp-includes/ms-files.php?file=2013/02/ Expanding-Evidence-Approaches.pdf

10 Faith Boninger and Alex Molnar. (2016). Learning to Be Watched: Surveillance Culture at School. *The Eighteenth Annual Report on Schoolhouse Commercializing Trends, 2014-2015*, National Education Policy Center, School of Education, University of Colorado - Boulder.

11 Ibid.

12 J. William Tucker and Amelia Vance. (2016). School Surveillance: The Consequences for Equity and Privacy. *Education Leaders Report* 2(4), National Association of State Boards of Education.

13 Lord, R. & Henney, M. (2015, August 20). Surveillance Society: Students easy targets for data miners. *Pittsburgh Post-Gazette*. http://www.post-gazette.com/news/surveillance-society/2015/08/20/Surveillance-Society-Students-easy-targets-for-data-miners/stories/201508230018

14 J. William Tucker and Amelia Vance.(2016). School Surveillance: The Consequences for Equity and Privacy. *Education Leaders Report* 2(4), National Association of State Boards of Education.

15 Information gathered on or before January 23, 2017.

16 Common Sense Education. (2016). Surveying Encryption Practices of Technology Used in Public Schools. https://www.commonsense.org/education/privacy/survey/encryption

17 J. William Tucker and Amelia Vance.(2016). School Surveillance: The Consequences for Equity and Privacy. *Education Leaders Report* 2(4), National Association of State Boards of Education.

18 See https://studentprivacypledge.org/.

19 See https://studentprivacypledge.org/signatories/ for a list of signatories.

20 The Pledge's 12 provisions as well as notes and definitions can be found at https://studentprivacypledge.org/privacy-pledge/.

21 33 C.F.R. Part 99.3.

22 Family Policy Compliance Office, U.S. Dept. of Ed., *Family Educational Rights and Privacy Act (FERPA)*, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html/.

23 Mark MacCarthy. (Dec. 2 2015). Some Misunderstandings of the Student Privacy Pledge. https://www.siia.net/blog/index/Post/62938/Some-Misunderstandings-of-the-Student-Privacy-Pledge/.

24 Google response to Sen. Al Franken. (Feb. 12, 2016). https://www.franken.senate.gov/files/letter/160216GoogleResponse.pdf

25 20 U.S.C. §1232g(a)(4).

26 33 C.F.R. Part 93.3.

27 Privacy Technical Assistance Ctr. Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. U.S. Department of Education, (2014) *available at* https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

28 33 C.F.R. Part 99.31.

29 Federal Trade Commission. (Last revised March 2015). Complying with COPPA: Frequently Asked Questions. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently- asked-questions

30 Ibid.

31 Data Quality Campaign. (2016). Student Data Privacy Legislation: A Summary of 2016 State Legislation. http://dataqualitycampaign.org/resource/2016-student-data-privacy-legislation/

32 Center for Democracy & Technology with BakerHostetler. (2016). State Student Privacy Law Compendium. https://cdt.org/insight/state-student-privacy-law-compendium/

33 Cal. Bus. & Prof. Code §22584 (2014).

34 C.R.S.A. §22-16-101 (2016).
35 An Act Concerning Student Data Privacy, Pub. Act. No. 16-189 (2016).
36 Privacy Technical Assistance Center. (2014). Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. U.S. Department of Education. https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf
37 Privacy Technical Assistance Center. (Revised 2016). Protecting Student Privacy While Using Online Educational Services: Model Terms of Service. U.S. Department of Education. http://ptac.ed.gov/sites/default/files/TOS_Guidance_Mar2016.pdf
38 See, e.g., Cambridge Public Schools' (MA) list of approved digital resources: https://secure2.cpsd.us/mspa/district_listing.php?districtID=457
39 See, e.g., https://ssd.eff.org/en/module/creating-strong-passwords *and* https://www.eff.org/dice
40 American Library Association. (Last updated January 2017). Library Privacy Checklist for Students in K-12 Schools. http://www.ala.org/advocacy/privacyconfidentiality/privacychecklists/library-privacy-checklist-students
41 American Library Association. (Last updated April 2016). Library Privacy Guidelines for Students in K-12 Schools. http://www.ala.org/advocacy/library-privacy-guidelines-students-k-12-schools
42 American Library Association. (Adopted January 2014). Developing or Revising a Library Privacy Policy - School Libraries. http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/Developing-or-Revising-a-Library-Privacy-Policy#schoollibrareis
43 See https://chooseprivacyweek.org/for-libraries/.
44 See Jeremy Gillula, Guide to Google Account Privacy Settings for Student. *Deeplinks*. (Dec 1, 2015). https://www.eff.org/deeplinks/2015/11/guide-google-account-privacy-settings-students
45 See Jeremy Gillula, Guide to Chromebook Privacy Settings for Students. *Deeplinks*. (Dec 1, 2015). https://www.eff.org/deeplinks/2015/11/guide-chromebook-privacy-settings-students
46 G Suite for Education Privacy Notice. https://gsuite.google.com/terms/education_privacy.html *and* Sophia Cope & Jeremy Gillula, Google Changes Its Tune When It Comes to Tracking Students. *Deeplinks*. (Oct 6, 2016). https://www.eff.org/deeplinks/2016/10/google-changes-its-tune-when-it-comes-tracking-students
47 Kamala D. Harris. (2016). Ready for School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data. California Department of Justice. https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/ready-for-school-1116.pdf
48 Privacy Technical Assistance Center. (2012). Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics: An Issue Brief. U.S. Department of Education. https://tech.ed.gov/learning-analytics/