Educator Toolkit

for Teacher and Student Privacy

A Practical Guide for
Protecting Personal Data

PARENT COALITION FOR STUDENT PRIVACY

BADASS TEACHERS ASSOCIATION

OCTOBER 2018

TABLE OF CONTENTS

INTRODUCTION & ACKNOWLEDGEMENTS 1

SECTION I: Why is teacher data at risk? 4

SECTION II: Why is student data at risk? 8

SECTION III: What teachers should know about federal student privacy laws 13

SECTION IV: Important points to consider before educators adopt education technology 20

SECTION V: Limit social media use in school with ten simple rules to follow 26

SECTION VI: Best practices and practical tips to protect teacher and student privacy 30

SECTION VII: How to advocate for stronger teacher and student privacy protections 33

APPENDIX A Sample teacher contract language protecting educator privacy 35

APPENDIX B Results from our educator survey, focus groups, and interviews on data privacy 36

- I. Online survey 37
- II. Focus groups 46
- III. Administrator one-on-one interviews 48
- IV. Online products used by respondents 50

RESOURCES 52

INTRODUCTION

Outraged teachers in West Virginia went on strike in the spring of 2018 because, among other reasons, they were being forced to download Go365, a wellness and rewards app which would track their steps and other health data. Failure to use the app or meet fitness goals would result in increases in their health insurance premiums and deductibles. Teachers were required to upload a variety of personal health information into the app and saw the program as an invasion of personal privacy. They fought back and won. The app was tossed out.

On the other hand, on June 27, 2018, the United State Supreme Court ruled on the case of *Janus v. AFSCME*, deciding that from now on, teacher union dues would be made voluntary. On the same day and for several weeks thereafter, teachers across the country reported receiving emails to their school addresses from various anti-union groups, asking them to fill out online forms to opt out of the union. Their email addresses had been made available through freedom of information requests, or because in many states, this information is already publicly available. The forms also required teachers to offer additional personal information, which would then allow these groups to create a comprehensive educator database, to be used for further solicitation and political organizing.

While these examples may seem extreme, the reality is that teachers and students throughout the United States have their personal data shared with dozens, if not hundreds, of technology companies, organizations, and government agencies over the course of a normal school year, seriously threatening their privacy.

So what is privacy and why does it matter? Privacy refers to the ability to protect one's own personal information and control with whom and how the information is shared. It matters because even if you're not doing anything illegal or feel you have nothing to hide, the standards and norms by which judgements are made about behavior that's "right" versus "wrong" today could easily change tomorrow. Moreover, the freedoms of expression, association, and assembly — all of which are necessary for a free and functioning democratic society — are underpinned by the right to privacy.

Teachers should care about privacy, especially given the massive amount of personal information collected about them and their students in the average classroom today. Consider for a moment the student data gathered by schools to track outcomes and teacher data collected for performance evaluations. In many cases, these data are sent to the district or the state education department for accountability purposes and are then shared with other governmental agencies and researchers. As education policies shift toward "workforce development" and "career pathways," this intricate web of highly sensitive data could impact individual teachers and students for life.

The growing use of of education technology or ed tech in schools only compounds the problem. If your school employs data dashboards, online grading books, web-based instructional systems, or classroom apps, or if your school assigns students to use laptops, digital devices, or social media networks, information about you and your students may be sent every minute to vendors and other third parties with insufficient oversight given to how the data will be used and secured. At the same time, federal laws aimed to protect education-related data are outdated and inadequate to protect school records in the digital age.

To better understand how educators perceive these and other complex privacy-related issues, the Badass Teachers Association and the Parent Coalition for Student Privacy surveyed and interviewed 365 teachers and administrators across the country. Seventy-four percent of teachers said they used classroom apps not required

by the district in which they have entered sensitive academic or behavioral student data, with little or no vetting of whether or how the app protects or secures this data, or even whether the app complies with federal or state privacy laws. And yet 68 percent of teachers who responded to our survey say they have received no training from their schools on how to use these systems to minimize the chances that personal data will be breached or abused.

This lack of training and support is of particular concern since schools across the country face growing threats to data security. Since January 2016, more than 350 cybersecurity incidents, which include data breaches and hacks, have been publicly documented by U.S. K-12 schools. In one extreme case, over 360,000 Pennsylvania teachers and retirees learned that their Social Security numbers, dates of birth, and home addresses stored on a state education department database had been accessible to unauthorized users.

A case that garnered national media attention occurred at the hands of a notorious hacker group called "The Dark Overlord," who broke into school data systems in Alabama, Iowa, Montana, and Texas, and threatened to release sensitive student information if ransom were not paid. As of January 2018, according to the FBI, The Dark Overlord was responsible for at least 69 unauthorized intrusions into the databases of schools and other businesses and had attempted to sell more than 100 million records involving the personally identifiable information of over 7,000 students.

Researchers and advocacy groups are also uncovering surreptitious ways in which companies are using student and teacher data for non-educational purposes. For example, in June 2018, the Fordham Center for Law and Information Policy published a study revealing a massive "marketplace" for student data available for purchase on the basis of "ethnicity, affluence, religion, lifestyle, awkwardness, and even perceived or predicted need for family planning services." The study documented an overall lack of transparency in the commercial marketplace and an absence of legal protections for student information.

Teachers are already overworked and under-resourced, so expecting them to address these complex and emerging risks to privacy on their own isn't reasonable. We're here to help. Whether you're new to the profession or a veteran, you can serve as an important gatekeeper to learn about and strengthen the safeguards against your students' and your own personal information from being extracted and exploited. Our toolkit uses plain language to walk you through some practical information about data privacy and the steps you should take to help protect it.

We hope you find this information useful and that it helps empower you to make the right choices for yourself and your students.

If your school or district is interested in professional development to help train teachers on how to protect their privacy and that of their students, please contact **Marla Kilfoyle** at ***TeacherPrivacy2018@gmail.com.***

ACKNOWLEDGMENTS

This effort was a joint project of the Parent Coalition for Student Privacy and the Badass Teachers Association, and was made possible by grants from the Rose Foundation for Communities and the Environment's Consumer Privacy Rights Fund, the American Federation of Teachers, and the NEA Foundation.

— Special thanks to Advisory Members —

Faith Boninger *- Co-Director of the Commercialism in Education Unit at the National Education Policy Center*

Jamaal Bowman *- Principal, CASA Middle School (NY)*

Carol Burris *- Executive Director of the Network for Public Education*

Andy Coons *- Senior Director, National Education Association Center for Great Public Schools*

Ronsha Dickerson *- Parent Advocate, Journey for Justice Alliance (NJ)*

Dr. Michael Flanagan *- Educator, New York City Department of Education*

Eileen Graham *- Parent Advocate, New York State Allies for Public Education (NY)*

Peter Greene *- Retired teacher and education writer (PA)*

Josh Hickey *- Educator, Oceanside School District (NY)*

Michelle Kasprzyk *- Library Technology Specialist, Pinella County School District (FL)*

Carrie Odgers Lax *- President, Ridgewood Education Association (NJ)*

Roxana Marachi *- Associate Professor of Education, San Jose State University and Education Chair, San Jose/Silicon Valley NAACP*

Chris Paschke *- Executive Director of Data Security, Jefferson County Public Schools (CO)*

Susan Polos *- Library Media Specialist, Bedford Central School District (NY)*

Steven Singer *- Educator (PA)*

Steve Smith *- Chief Information Officer, Cambridge Public Schools (MA)*

Robin Vitucci *- American Federation of Teachers, Education Issues*

— Disclaimer —

While the goal of this toolkit is to provide valuable resources to help you protect teacher and student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your particular situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

The graphic illustrations appearing in this toolkit were originally created for the Parent Toolkit for Student Privacy, produced by the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood.

Graphic images appearing in Appendix B were created by the Badass Teachers Association graphics team.

SECTION I:
Why is teacher data at risk?

You may be asking yourself, why should teachers be worried about their data? After all, we volunteer our personal information all the time — when we are posting pictures on social media or ordering pizza through an app on a smartphone.

The answer is simple: your data reveals a lot about you, and its release may impact your reputation, livelihood, and civil liberties. Indeed, there is growing consensus that "Big Data" — a term used to describe the process by which extremely large data sets are analyzed to reveal patterns and correlations — can have an adverse effect on members of society. The Data Justice Lab at Cardiff University mapped at least six ways in which Big Data is inflicting harm: targeting individuals based on vulnerability, misuse of personal information, discrimination, data breaches, political manipulation, and system errors that can lead to inaccurate identification or loss of benefits, such as government assistance programs.

The education sector isn't immune to these issues. In part because the U.S. spends approximately $650 billion per year on K-12 education and global investments in educational technology have risen to $9.5 billion, education is poised to serve as a data-rich environment from which policy decisions and corporate fortunes are made. At a White House event in 2012, the CEO of Knewton, an international "adaptive learning technology" company, candidly admitted that "education happens to be today the world's most data-mineable industry by far, and it's not even close." Here's how.

Teachers generate a lot of data

You might be surprised how much data teachers produce. There are demographic and administrative data that teachers must provide that the school or district collects as a condition of employment. These generally include your name, address, date of birth, photo, Social Security number, licensure or certification information, courses taught, W2 and banking information, performance data, health conditions, education credit information, and work record.

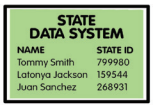
Teachers also create and share some of their own data with private companies when they use technology tools in the classroom, particularly if they're issued personal laptops or devices by the school or district. These data may include their names, email addresses, schools, photos, courses or subjects taught, lesson plans and tests they created, internet use, geolocation, email correspondence and social media posts, and "metadata," or data about data that provide meaning and context, including their search engine queries, website visits, and much more.

Teacher data is profitable

In May 2017, *The Economist* declared that data has replaced oil as the most valuable resource in the world. Not surprisingly, some of the most profitable companies in the U.S. and abroad deal in data, including many used in schools such as Alphabet (Google's parent company) and Facebook. Have you ever wondered why these giants and other companies can offer their services for free? It's simple. Profiles are generated based on user interests, purchasing habits, and online behavior, which are then used for advertising and redisclosed to other third parties for unregulated use.

According to a report released by Common Sense Education in May 2018, ten percent of the hundred "most popular applications and services used in educational technology" indicate that they "may create and target profiles of their users," which can ultimately be used for commercial purposes.

> Khan Academy, the free online instructional video platform widely used by teachers and students, explains in its Privacy Policy, dated May 25, 2018, that it participates in "interest-based advertising" and uses "third party advertising" to track users and serve them targeted ads across other websites and social networks like Facebook.



Teacher data can be used for high-stakes decision-making

As of 2015, every state except California, Iowa, Montana, Nebraska, and Vermont utilized student scores on standardized exams to evaluate teachers. In most cases, teacher evaluations are determined by complex formulas based on these test scores in conjunction with other factors, including how well technology is utilized in the classroom. The algorithms or systems behind these models are often secret or so complex to be impossible for outside sources to validate. Yet the results can often be used in high-stakes decisions, including tenure and employment terminations.

> In 2017, the Houston Federation of Teachers sued the Houston Independent Schools in federal court over the district's controversial Education Value-Added Assessment System (EVAAS). A federal judge ruled in favor of the teachers, stating that "high stakes employment decisions based on secret algorithms [are] incompatible with due process." The judge declared that the proper remedy was to reverse the policy.

Teacher data is shared with state education departments and beyond

When your school or district gathers data about you, the information is often sent to the state, linked with data from other sources, and housed in databases to track your professional performance, for the purpose of research or policy-making. This information may then be used to identify supposedly "underperforming" teachers and schools. Many state data systems link teacher names, ID numbers, district codes, school codes, and course titles with individual student names, ID numbers, grade levels, and final grade/course completion status. According to the Colorado Department of Education's website, this information is used, among other purposes, to help the state answer such questions as "How are the students in X's class performing?"

> An elementary school teacher sued New York state education officials in 2014 over her "ineffective" rating churned out by the state's controversial VAM teacher evaluation system. A State Supreme Court Judge rendered the rating void in 2016, citing the teacher's rating as "arbitrary and capricious."

Teacher data is vulnerable to exploitation

It's no small task to properly secure data: it takes money, staff, resources, training, and sustained commitment. As schools struggle to stretch their shrinking budget dollars, prioritizing data security often falls short, leaving sensitive teacher information vulnerable to accidental breaches and deliberate hacks. Since 2016, U.S. K-12 public schools have reported more than 370 cybersecurity incidents, according to EdTech Strategies, a research and consulting firm.

"Phishing scams" are one of the most common threats to educators, in which scammers attempt to obtain confidential employee information by posing as a trustworthy entity in an email. Victims of these and other deceptions can spend thousands of dollars to reverse identity theft. Some may never fully recover.

> The K-12 Chief Information Officer at the Kentucky Office of Education Technology testified to Congress in May 2018 that four billion attempted attacks had been launched against Kentucky's education data infrastructure over the last academic year. Phishing attacks, he reported, had increased 85 percent and were increasingly more sophisticated, targeting "relevant officials."

> In January 2017, a payroll employee of the School District of Manatee County (FL) fell victim to a phishing scam and released confidential W2 tax information, including Social Security numbers, of 7,700 district employees.

> In February 2017, the Internal Revenue Service issued a warning to schools about a phishing scam targeting payroll departments at more than 20 school districts across the country.

Survey Results:

In response to our survey, 84 percent of teachers said they had never had training to prevent cyberattacks or breaches of personal data, and 45 percent reported that student and teacher privacy were never discussed at faculty meetings.

Teacher data can be extremely sensitive and personal

School districts across the country are beginning to utilize wellness programs in an attempt to boost productivity and reduce employee healthcare costs. To monitor individuals' baseline health and behavior, some programs use online health tracking apps to collect sensitive medical information, including teachers' blood pressure and cholesterol levels, prescribed medications, pulse rates, steps taken, and other physical activities. Many teachers find these programs to be an invasion of privacy, contributing to the outrage of those who went on strike in West Virginia in spring 2018.

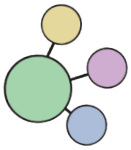
Teacher data can be repurposed

Privacy Policies and Terms of Service (TOS) of many popular ed tech companies claim the right to use and disclose teacher and student data to their affiliates and other entities, or repurpose it in various ways, including to help them improve or develop new products. You should be aware that just because a website or app is advertised as an ed tech tool, it doesn't necessarily mean the personal data collected will be treated any more responsibly than data collected by apps designed for typical consumer use.

Teacher data can stay online indefinitely

Your data can quickly spread beyond your control. Every piece of information you or someone else shares about you, whether a blog post of your political musings, a picture of you at Saturday's barbecue uploaded to social media, "likes" on a friend's post, or clicks on a vendor's ad, can follow you for years. Even if you delete content or close your accounts, don't assume the information has disappeared; it may still be stored by the host company, by other companies that have scraped the information off the web, or by someone who captured a screenshot.

> Teachers make mistakes; they're human after all. But it is possible to reduce the risk by taking special precautions not to express your views about individual students or post comments on social media platforms that may be perceived as offensive. In 2017, an Ohio teacher was placed on leave after criticizing students on Snapchat for spending money on their prom while complaining of not "having enough money for school supplies or passing grades."



Teacher data ownership can be unclear

Many ed tech products rely on user content to operate as intended. For example, teachers using Kahoot! upload quizzes, photos, and videos to create learning games played by their own students and others. Kahoot!'s Terms of Service claims that users retain their intellectual property rights to their uploaded materials but also that the company is granted a "perpetual (or, for as long as permitted under applicable law), non-exclusive, sub-licensable, transferable, royalty-free, irrevocable, fully paid, universal license to commercialize, use, reproduce, make available to the public (e.g. perform or display), publish, translate, modify, create derivative works from, and distribute any" user content. Basically this means that by using Kahoot! you agree to allow the company to use, reuse, and sell anything you upload to their system, anywhere in the world, without paying you or asking your permission.

> The Summit Personalized Learning Platform, an online program developed by Summit charter schools in collaboration with the Chan Zuckerberg Initiative (CZI), initially claimed all rights to teacher work and assignments as a condition of all Summit public and charter schools that used their platform. This is still the default position. If teachers don't opt out, their assignments and all other intellectual property are automatically shared with the Summit operators and CZI.

SECTION II:

Why is student data at risk?

Like teacher data, student data is under threat now more than ever before. Schools are collecting ever-increasing amounts of information to comply with accountability measures imposed by the state and federal governments. At the same time, digital tools are being introduced in our schools at breakneck speed, often without careful consideration of how the copious data collected as part of their implementation will be used and safeguarded.

Compounding the problem, the primary federal education law protecting personal student information, the Family Educational Rights and Privacy Act (FERPA), is more than 44 years old, has never been updated to address new security and access threats presented by the digital collection and storage of student records, and has been weakened over time to allow even more disclosures of data to third parties without parental knowledge or consent.

Understanding what data is being collected and the risks involved is the first step teachers should take to protect students and their privacy. Read on to learn more.

Students generate a lot of data

Over the course of their educational career, students produce enormous amounts of data. When students enroll in school, their parents must provide demographic and administrative data including their children's names, addresses, dates and countries of birth, family and residency information, and medical conditions. Additionally, schools collect students' photos, course grades, test scores, behavior incidents, disabilities, special education accommodations, disciplinary data, racial and economic status, languages spoken at home, and much more.

Students also create and share a subset of data with private entities when they are assigned to use technology at school, whether for instruction, assessment, or other monitoring purposes. These data can include their names, schools, school addresses, email addresses, photos, course schedules, behavioral information, grades, test and survey answers, internet searches, and metadata – meaning data about data, such as their usage of the product, including where and for how long they delay answering questions or other website behavior.

Additionally, since technology is integrated into nearly every aspect of a child's education, other sensitive information may be collected, including their fingerprint images for tracking lunch purchases; heart rate data and other health information amassed by fitness trackers in gym class; voice recordings stored by digital reading tools; behavior and disciplinary incidents logged into online classroom or school management tools; and research and term papers submitted to programs used for plagiarism detection or editing.

Student data is profitable

It was once believed that student data was a low-value target for hackers and criminals, simply because it did not contain bank account or credit card numbers. Yet because few children have negative credit histories and because student data can include Social Security numbers and their mother's maiden names, hackers are eager to acquire student data to steal their identities.

> A child's Social Security number can be sold for $25 to $35 on the dark web, and the data from the students at just one school can be worth more than $10,000.

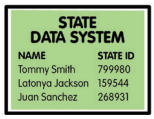
Student data is also valuable as a corporate asset. Some state laws and even the Student Privacy Pledge, a voluntary set of data principles agreed upon by 347 ed tech companies as of June 2018, specifically allow private corporations to sell student data — worth millions — in the case of mergers, acquisitions, and bankruptcies. Other companies, including the College Board (which owns the PSAT and SAT) and ACT, sell or "license" students' profiles to colleges and companies containing their personal data, which they gather through surveys before test administration. As of 2018, the College Board charged these organizations and companies $0.43 per individual student name and profile.

The U.S. Department of Education recently warned states and districts that assign students to take these exams during the school day to obtain prior parental consent agreeing to these and other disclosures of student data or they risk violating several federal privacy laws, including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Individuals with Disabilities Education Act (IDEA). See Section III for detailed information.

> According to a recent Fordham Center for Law and Information Policy report, researchers identified 14 data brokers, including American Student Marketing, Exact Data, and Scholarships.com, who "conclusively sell or advertise the sale of student information or have done so in the past."

Another potential threat to student data is led by philanthropic and investment banking sectors poised to fund public services through the use of "Social Impact Bonds" and "Pay for Success" programs. In short, bankers or foundations may be interested in financing projects aimed to serve the public good, such as reducing juvenile recidivism or boosting early learning, and be paid back if certain metrics are subsequently met to indicate "success." The evidence of the "success" of these programs typically involves collecting and tracking children's personal data.

> In 2015, one of the nation's first Social Impact Bond partnerships between Goldman Sachs and a Utah preschool program resulted in the payout of $260,000 in public dollars to the Wall Street investment bank. Despite criticisms from nine early-education experts of the program's methodology, the project was considered successful when 109 allegedly "at-risk" preschoolers were tracked and found to have avoided costly special education intervention in kindergarten.



Student data can be used for high-stakes decision-making

Because more and more data concerning student activities, behavior, and ability is being collected at earlier ages, some companies are generating "profiles" using predictive analytics to forecast their future behavior. For example, many companies sell "early warning tools" that profess to predict which students are "at risk" of not graduating, using attendance, achievement, and/or behavior data as indicators. Teachers can track student progress over time via a mobile-ready or desktop dashboard. It's not difficult to imagine how this data could falsely identify certain students, limit their ability to enroll in certain courses, or even cause schools to push them out by encouraging them to transfer to other schools. There is also the very real potential of teachers absorbing negative data through these dashboards and creating negative stereotypes of their students that could hamper their future success.

Student data is shared with state education departments and beyond

When student data is collected by schools, it's often sent to the state education department and tied to individual teacher data for the purpose of tracking "teacher effectiveness" or other policy initiatives. Student data can also be linked to data sets from other state agencies, including the departments of higher education, health and human services, and workforce development, to be used for longitudinal research, evaluation, and policy-making.

Many schools collect sensitive data related to students' country of birth and date of entry into the United States and share this information with the state. Though schools are not supposed to ask the documentation status of any student, this information could then be used as a proxy or screening device if the state or federal government decided to access it for this purpose. Similarly, disciplinary and arrest records of students are collected by schools and may be used against them and prejudice their futures.

> In June 2018, Boston Public Schools Superintendent Tommy Chang resigned his position shortly after a lawsuit was filed by civil liberty and advocacy organization that accused district officials of sharing school police reports with federal authorities, resulting in the arrest and deportation of a former undocumented student. While Chang insisted the student's immigration status was never revealed, advocates urge schools to use caution when cooperating with law enforcement, particularly in investigations in which Immigration and Customs Enforcement (ICE) may be involved.

Student data is vulnerable to exploitation

All education data is at risk of cyberattacks, and a special kind of hacking called ransomware is emerging as a particularly serious threat to students' online and physical safety. In a typical ransomware attack, a hacker or group of hackers seize control of a student information system of a school or district. They then block administrators' access to the system and threaten to disclose personal student data unless paid a substantial amount of money.

In fall 2017, a group known as The Dark Overlord took ransomware attacks to new levels by breaking into school data systems in at least four states and threatening to release student records if their demands weren't met. Some students were further victimized when the hackers sent them threatening text messages, including a specific reference to "splatter kids' blood in the hallways." In response to this and similar cyberattacks, the U.S. Department of Education issued guidance, warning school districts of a "New Type of Cyber Extortion/Threat" and giving specific advice on how to protect against such attacks. To access this and other guidance released by the Department, see the Resources section.

Student data can be extremely sensitive and personal

Authorized by Congress in December 2015, the federal education law known as the Every Student Succeeds Act encouraged states to broaden their definition of academic success, freeing up federal funds to develop and measure students' social and emotional learning (SEL). As a result, according to a June 2018 *Education Week* report, think tanks, philanthropic organizations, and venture-capital firms are investing hundreds of millions of dollars to support and eventually take advantage of the new opportunity.

To measure how students feel and to track their SEL growth, some ed tech companies are developing surveys and databases to capture their "grit" and "growth mindset." In other cases, as reported by *Education Week*, researchers are using student biometric data collected by "facial recognition, eye-tracking, wearable devices, and even virtual reality" technology to monitor how students are feeling.

> According to *Education Week*, Spokane Public Schools in Washington uses the data analytics company Panorama Education to administer surveys to students with questions such as, "In school, how possible is it for you to change how easily you give up?" Answers to each question are analyzed by Panorama, assigned a 0–5 score in areas of "grit, growth mindset, and social awareness," and stored in the company's database.

Student data can be repurposed

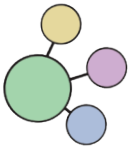
Unfortunately, it's not at all uncommon for ed tech companies to commercialize or otherwise use student data for their own purposes. At least twenty-two states, including California, Colorado, Illinois, and Virginia, have recently passed state laws specifically allowing ed tech companies that collect students' personal information for "school purposes" to also utilize the data without parental consent to develop and improve their products and services. A student's intellectual labor should be used strictly to benefit the individual child, not for companies to profit from.

> At a spring 2018 conference, education giant Pearson announced it had inserted "social-psychological interventions" into its learning software without permission from the colleges utilizing the software or their students. Over 9,000 students at 165 colleges and universities were unwitting subjects in these experiments, designed to allow Pearson to use their data and metadata – not for their benefit, but to improve their products.

Student data can stay online indefinitely

Just like adults, students are still learning how the information they share publicly via social media or other online platforms can be abused. Even when they think their posts are private, it can be a hard lesson to find out that Big Brother is watching. Students should be aware that in many districts, administrators may be tracking their social media activity for "security" purposes, and college admissions officers may be monitoring their social media accounts to decide whether to admit them.

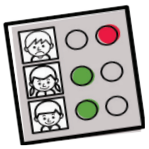
> In a 2018 report conducted by Kaplan Test Prep, 68 percent of surveyed colleges say it's "fair game" to use information gleaned from applicants' social media accounts to determine who gets accepted.



Student data ownership can be unclear

Companies offering ed tech apps and websites commonly assigned by teachers can claim certain rights to student content in their Terms of Service. For example, "grammar check" programs such as Grammarly and services used to "improve student writing," such as Turnitin, grant the companies and their subcontractors a "non-exclusive, worldwide, royalty-free and fully-paid, transferable and sublicensable, perpetual, and irrevocable license to copy, store

and use" user content. This means that any papers or other content uploaded by students can be republished, provided to third party affiliates around the world, and used any way these companies wish, without any payment to the student. Most students are too young to understand what consequences might arise from such an agreement.



Student data can be used to stereotype

When educators over-rely on secondhand information about students' past academic or behavior records, this may lead to self-fulfilling prophecies. If teachers hear that students have excelled in the past or are predicted to do so in the future, research shows that even if that information is false, it tends to lead to more investment in those students, which enhances their chance of success. This is called the "Pygmalion effect." Conversely, if teachers learn that their students have spotty histories, either in terms of their grades or behavior, they may suffer from the "Golem effect," causing teachers to lower their expectations and disengage, which may in turn cause their students to struggle even more.

Survey Results:

Ninety percent of our teacher survey respondents reported that their district uses student information systems or data dashboards, and that teachers enter personal student information on a daily or weekly basis to track grades, attendance, enrollment, suspensions, and other sensitive issues.

Several of our survey respondents worried that this data collection could create a scenario where teachers might have preconceived ideas about their students before they met them based on accessing their discipline or academic histories, and which could lead to self-fulfilling prophecies.

In general, there was a consensus that, as one administrator observed, "We need to find the balance between technology and teaching." As another commented, "Technology is moving too fast. Districts are struggling to keep up."

SECTION III:
What teachers should know about federal student privacy laws

One way for teachers to protect themselves and their students is to understand their responsibilities under federal law. There are five major federal laws governing the use and disclosure of a student's personal information: **FERPA** (Family Educational Rights and Privacy Act), **NSLA** (National School Lunch Act), **IDEA** (Individuals with Disabilities Education Act), **PPRA** (Protection of Pupil Rights Amendment), and **COPPA** (Children's Online Privacy Protection Act). In each case, we will provide practical examples of how the laws apply to you as an educator.

Additionally, 39 states plus the District of Columbia have passed student privacy-related education laws since 2013. A few of these laws also have specific provisions that protect teacher data. For example, New York passed a law in 2014 prohibiting the disclosure, sale, or use of educator evaluation data for marketing purposes by districts, third-party contractors, or their assignees. In 2017, New Hampshire passed a law preventing teachers from being video recorded during evaluations without written consent of the teacher as well as the parents of each affected student. To learn more about your state's privacy laws, refer to the Parent Coalition for Student Privacy and Network for Public Education's *State Student Privacy Laws: A 50 State Report Card,* to be released in November 2018.

It's important to note that individual school districts may have policies in place that limit the sharing of student information beyond what state and federal law requires. Educators should contact their local boards of education to learn about local policies that may place additional protections for student or teacher privacy.

If you witness or experience what you believe to be privacy violations described in this section, first contact your union and then school administrators, your district, or the state department of education. You can also contact the Privacy Technical Assistance Center of the U.S. Department of Education to ask for advice as to how to proceed, or reach out to the advocacy organizations concerned with student privacy listed in Section VII.

Family Educational Rights and Privacy Act (FERPA)
(20 U.S.C. § 1232g; 34 CFR Part 99)

The Family Educational Rights and Privacy Act (FERPA) became law in 1974 and applies to schools receiving federal funds. Administered by the U.S. Department of Education, FERPA is the broadest federal law regulating student privacy, but in many ways it has been weakened to allow for the increased sharing of personal student data rather than strengthened for the digital age.

FERPA protects personally identifiable information (or PII) contained in student education records. Protected PII includes, but is not limited to, a student's name; the name of the student's parent or relatives; physical address; Social Security number or student ID number; biometric record; date of birth, place of birth, and mother's maiden name; or other information that, alone or in combination, would allow others to identify the student. Education records include, but are not limited to, grades, transcripts, class lists, student course schedules, health information, and student discipline data.

The general rule is that schools and teachers cannot disclose student PII — whether orally, written, or in electronic form — from education records without first obtaining permission from parents. However, the following exceptions have been incorporated into FERPA to allow for data disclosure without parental consent:

"DIRECTORY INFORMATION" *exception:*

Directory information is a limited set of information from students' education records that is not considered highly sensitive or an invasion of privacy if disclosed, including their names, addresses, phone numbers, date and place of birth, participation in school activities and sports, awards and recognitions, and dates of attendance. Schools may disclose students' directory information to third parties without parental consent if public notice has been provided to parents containing the types of information designated as "directory information," a statement of a parent's right to restrict or opt-out of its disclosure, and the period of time in which parents may exercise this right. Directory information is traditionally shared with school photography and yearbook companies, but schools are increasingly using this exception to upload class lists and share other student data to ed tech companies. See Scenario 1 below for more detail.

"SCHOOL OFFICIAL" *exception:*

Schools may disclose student PII from education records without parental consent to other "school officials," including vendors, consultants, contractors, and volunteers with "legitimate educational interests" performing "institutional services or functions" for the school. However, those designated "school officials" must meet certain conditions, including being under the "direct control" of the school, which may require a contract or other written agreement. They must also not use the data for any purpose not authorized. Many school vendors and other contractors often receive and collect student information without parental consent under the "school official" exception. See Scenario 1 for more detail.

"AUDIT AND EVALUATION" *exception:*

Disclosure of student PII in education records is also allowable without parental consent to "authorized representatives" of "Federal, State, and local educational authorities conducting an audit, evaluation, or enforcement of education programs." Under this exception, student data is often disclosed without parental consent to the state department of education and related agencies, or to other "authorized representatives" designated by a district, as long as there is a written agreement restricting the use of the data for that purpose.

"STUDIES" *exception:*

A fourth exception allows disclosures of student PII in education records without parental consent to organizations or individuals for "studies." These studies must be limited to the purpose of "developing, validating, or administering predictive tests; administering student aid programs; or improving instruction." Again, there must be a written agreement restricting the use of the data for this purpose before this disclosure can occur. This exception is generally used when schools disclose student information without parental consent to researchers or testing companies.

Scenario 1

Q: I want to use a free app that allows me to award points to students for good classroom behavior. After creating a teacher account, the app is asking for student names, class periods, and photos. Does FERPA allow me to share this information?

A: First, has your school or district vetted this app for compliance with state or federal privacy law? If not, you must be very careful. Best practice in any case is to obtain district, school, and parental consent before using any app that collects personal student information.

Should you decide not to seek parental consent, FERPA allows schools to disclose a limited set of student data with third parties under the "directory information" exception. If you intend to use this exception, make sure any information you load into the app aligns with the types of information your school or district designates as directory information. See above for more details. You should also verify whether any parents have opted-out of disclosure of their child's directory information. Otherwise, you could be violating FERPA.

The "school official" exception may also apply in this case but only if the app meets certain criteria. First, the app must have a "legitimate educational interest," perform an "institutional service or function" on behalf of the school, and be under the school's "direct control." Check with your school or district to make sure the app is meeting each of these conditions. It's important to note, however, that the U.S. Department of Education suggests that a good method to determine whether the app company is under the school's direct control is to read the Terms of Service (TOS). For example, if the app provider claims it may change the terms at any time without notice to you, the user, this may violate FERPA.

If the TOS allows for personal data to be used for non-educational or commercial purposes, this may also violate FERPA. Finally, if your students are under the age of 13 and will be entering personal information themselves into the online app, additional restrictions may apply. For more information, see the Children's Online Privacy Protection Act (COPPA) section on page 18.

Scenario 2

Q: My school uses a "data wall" to group students by assessment scores or academic progress. It's posted in a main hallway of the school. Does this violate FERPA?

A: If a data wall is visible to the public, and information displayed includes student names or other information that could identify them, along with their test scores or grades or other personal information from their education records, the data wall is likely in violation of FERPA. If you must use data walls, remove any identifying student information and/or ensure they are located in a private space such as the principal's office. For more reasons why data walls may do more harm than good, see relevant articles listed in the Resources section.

Scenario 3

Q: Our administration sends out a weekly newsletter to the entire school staff with announcements and other important information. One section names students who have been suspended and the reason for the suspension. Is this in violation of FERPA?

A: Yes! Personally identifiable information or PII contained in a student's education record, including disciplinary information, should be made available only to those school staff members who are directly involved in a child's education. This applies also to school staff who may be able

to view this information through student databases or information systems, such as Infinite Campus or PowerSchool. Only school employees with a "need to know" should be provided access to personal information in the student's education records, including digital data.

Individuals with Disabilities Education Act (IDEA)

(Public Law No. 94-142)

The Individuals with Disabilities Education Act (IDEA) is designed to protect the rights of children with disabilities, including students with Individualized Education Programs or IEPs, who are to be provided with a free and appropriate education.

The law is administered by the U.S. Department of Education and gives parents the right to consent before their child's PII can be disclosed in the following circumstances: 1) to participating agencies providing or paying for transition services used to facilitate a child's movement from school to after-school activities; 2) when a public-school child with disabilities intends to enroll in a private school in a different district from the parents' residence; and 3) each year before the district can disclose special education service records for reimbursement from the federal government.

Scenario 4

Q: A parent requested that all information relating to her child's Individualized Education Program (IEP), including updates and progress reports, be sent to her via email. Does IDEA allow this?

A: Parents may receive email copies of their child's IEP and progress reports if:

1) the school obtains prior parental consent;
2) the parents provide their confidential email address;
3) a secure password is used to access documents;
4) hard copies are provided upon request; and
5) parents may refuse the email option at any time.

National School Lunch Act (NSLA)

(79 P.L. 396, 60 Stat. 230)

The National School Lunch Act (NSLA) became law in 1946 and is administered by the U.S. Department of Agriculture (USDA). It protects confidential information collected by schools used to determine whether a child is eligible to receive free or reduced-priced lunch (FRL) or free milk under the National School Lunch Program.

In general, NSLA requires prior parental consent before FRL eligibility information, including household size and family income, can be shared with parties inside or outside of the school. Only school officials directly responsible for the child's education should be allowed access to eligibility status (whether they are eligible for free meals or free milk or reduced-price meals), and schools must make efforts to prevent "overt identification" of a child's FRL status.

Scenario 5

Q: Students receiving FRL at my school are given color-coded lunch tickets, and their purchases are tracked on a paper spreadsheet posted next to the cafeteria register. Does NSLA allow this?

A: No. NSLA prohibits "overt identification" of students' FRL status. Schools must make efforts to mask or otherwise de-identify a student's eligibility status to prevent others — especially other students — from viewing or accessing it. To prevent overt identification, schools should be sure not to publicize eligible families' or children's names. Schools should not have have separate dining areas, service times, or serving lines, or use any other method including colored meal cards, tickets, or tokens that could be used to differentiate students receiving free or subsidized meals.

Protection of Pupil Rights Amendment (PPRA)

(20 U.S.C. § 1232h; 34 CFR Part 98)

The Protection of Pupil Rights Amendment (PPRA), enacted in 1978, is administered by the U.S. Department of Education. PPRA requires schools to provide direct notice to parents of the right to refuse their child's participation in certain activities, at least annually at the beginning of the school year, and when the following activities may occur:

"MARKETING SURVEYS:"

Marketing surveys involving collection, disclosure, or use of personal information obtained from students for marketing purposes or to sell or "otherwise distribute the information" to others.

"EXAMS AND SCREENINGS:"

Non-emergency, invasive physical exams or screenings of students administered by the school, which are unnecessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings.

"SURVEYS, ANALYSES, AND EVALUATIONS:"

Surveys, analyses, and evaluations administered to students that are not federally funded and concern any of the following eight sensitive areas:

- Political affiliations or beliefs of the student or the student's parent;
- Mental and psychological problems of the student or the student's family;
- Religious affiliations and beliefs;
- Sex behavior and attitudes;
- Illegal, anti-social, self-incriminating, and demeaning behavior;
- Critical appraisals of close family members;
- Legally recognized privileged relationships, such as those of lawyers, physicians, and ministers; or
- Income (other than that required by law to determine eligibility for a program).

If any survey, analysis, or evaluation that deals with issues listed above is funded in whole or in part by a program of the U.S. Department of Education, parents must provide prior consent before their children are given these surveys.

Additionally, parents have the right to inspect the content of any surveys described previously, as well as any "instructional content that is provided to a student, regardless of its format, including printed or representational materials, audio-visual materials, and materials in electronic or digital formats (such as materials accessible through the Internet). The term does not include academic tests or academic assessments."

Scenario 6

Q: My school's counseling department intends to administer a survey to students about their drug and alcohol use. Does PPRA allow this?

A: Before administering a student survey that asks questions related to any of the sensitive areas listed on the previous page, schools must provide parents direct notice of when the survey will occur and an opportunity to view it and opt-out of their children's participation. If the survey is funded by a program of the U.S. Department of Education, parents must give prior consent. In general, schools should make every effort to ensure students' answers to surveys of any kind are confidential. Electronic surveys requiring students to log in with their name or student number are not considered anonymous. Survey tools like Google Forms or SurveyMonkey may provide some anonymity, but only if the privacy settings are utilized correctly.

Scenario 7

Q: Our state recently adopted the College Board's SAT college entrance exam as the mandatory annual state standardized test. On test day, students are instructed to complete a pre-exam survey asking questions about their religious affiliation and parental income. Is this allowed?

A: Historically, students taking college entrance exams did so voluntarily, and they registered and paid for the test themselves or with their parents' assistance. More recently, states and school districts are administering the PSAT, SAT, or ACT to all eligible students during the school day. In this case, schools pay for the exam and register students with the testing companies on their behalf.

The U.S. Department of Education's Privacy Technical Assistance Center recently issued guidance instructing states and school districts administering college entrance tests in this manner to notify parents and obtain their written consent before asking students questions that relate to religion, income, or other sensitive information covered under PPRA. Schools must also obtain prior written parental consent if student PII, including test scores, test score ranges, or demographic information is disclosed by the testing companies to third parties. Failure to do so can result in a violation of FERPA and IDEA. For a link to the Department's important guidance documents, see the Resources section.

Children's Online Privacy Protection Act (COPPA)

(15 U.S.C. 6501-6505)

The Children's Online Privacy Protection Act (COPPA) was enacted by Congress in 1998 and is enforced by the Federal Trade Commission (FTC).

COPPA regulates the activity of "operators" of child-directed websites, including education-related online programs or applications that collect, use, or disclose personal information collected online directly from children under the

age of 13. In general, COPPA requires operators to obtain parental consent prior to collecting children's personal information from them — including a child's name, email, phone number, screen name, geolocation, photo, voice recording, or other persistent unique identifier — and provide clear and prominent use of its data disclosure practices on its website.

Yet the FTC allows schools and teachers to act as a parent's agent and provide consent on their behalf — but only where the operator collects student's personal information for the use and sole benefit of the school and for no other commercial purpose.

When schools or teachers consent on behalf of parents, the FTC requires operators to provide the school notice of disclosure practices, as mentioned above, and the right for the school to request that the operator delete students' personal information and cease further collection or use.

Scenario 8

Q: My elementary school has a 1:1 program where each student is provided her/his own laptop. Teachers are encouraged to find education-related apps and load them directly to the devices. When I find one I like, I create a teacher account, agree to the app's Terms of Service (TOS), and assign my students to use the program, which then collects their personal data. Does this violate COPPA?

A: As explained in Scenario 1, your school or district should be vetting any technology that collects personal student information, including programs with "click-wrap" agreements where the user merely checks a box agreeing to the TOS before using an app. Whether or not your school or district has evaluated the product for compliance with federal and state privacy laws, best practice is to first obtain parental consent.

If you intend to provide parental consent on behalf of your students' parents, COPPA requires that the operator of the online program collecting their personal information uses it solely for the benefit of the school and not for any commercial purposes. The only way to know how an operator intends to use students' information is to read the TOS and Privacy Policy, which are typically long, confusing, full of jargon, and sometimes contradictory. COPPA doesn't provide a definition of "commercial purposes" and the FTC's guidance on this issue is limited, so it's up to schools and teachers to interpret whether they can act on a parent's behalf to provide consent.

SECTION IV:
Important points to consider before educators adopt education technology

Education technology can take many forms. It includes physical hardware such as computers, laptops, digital devices, and the wiring and routers needed to go online. It also includes software, such as word processing programs, student information and learning management systems, email and online document cloud storage programs, so-called "personalized learning" software, instructional and assessment programs, and free websites and apps.

Policies and practices for acquiring ed tech are varied across the country. What one educator may find in California could be very different in New York. When personal teacher and student data is made available to an ed tech company — whether the choice to do so was made by the district, school, or an individual teacher — the following guidelines are important to consider.

- **ENSURE** that any proposed product or service actually supports or improves teaching and learning.
- **MAKE ALL DECISIONS** to adopt ed tech programs in an open and collaborative manner.
- **ESTABLISH** that neither you nor anyone else making the decision is ethically compromised by having a personal or economic interest in the purchase or use of the program or app.
- **BE CERTAIN** that if you are making the decision, you are following school and district guidelines, as well as state or federal law.
- **CONSIDER THE HEALTH EFFECTS** on your students that may result from increased exposure to technology.
- **ED TECH CAN BE EXPENSIVE**; remember if it seems free, you are likely paying with either your and/or your students' personal data.
- **BE WARY OF "ADAPTIVE" OR "PERSONALIZED"** ed tech products using secret, company-owned algorithms that stratify students and direct them toward different paths based upon their responses.
- **VERIFY** that the ed tech company's data use and security practices are robust and adhere to federal and state guidelines.
- **WHEN IN DOUBT, ASK FOR PARENTAL CONSENT** before adopting any online program that allows for the disclosure of personal student data outside the school walls.

Educational or pedagogical value

The first and perhaps most important step to take before adopting ed tech is to evaluate whether the program will support or improve teaching and learning, rather than replace the relationship between you and your students. Confer with appropriate staff, including curriculum specialists, technology directors, school administrators, and other teachers in your subject area or discipline to obtain their opinion on the value that the program may bring to your classroom. The decision to utilize technology should not merely depend upon whether or not it frees up your time but whether it enhances learning opportunities for your students.

Also look for rigorous research to show that the program will actually deliver the results promised. Ed tech companies often make inflated claims about the efficacy and value of their products, and many media outlets and

organizations funded by ed tech corporations promote the use of these products without adequate proof in research or experience. Before implementing a digital product or service, check to see if there has been any independent study or evaluation done showing that it actually works to improve student outcomes.

In general, there is little research that supports the current rapid proliferation of ed tech or the claim that these products really "personalize" learning, according to a report by the Network for Public Education, *Online Learning: What Every Parent Should Know.* As the report points out, "Vendors often inflate claims for their products with self-serving studies of questionable quality or those commissioned and paid for by 'consultants.' Many students tend to become bored and disengaged and fail to learn critical communication skills and critical thinking when there is too little time devoted to human interaction and too little feedback offered by their teachers and fellow students." You can find a link to the full report in the Resources section.

Open decision-making

Decisions to acquire ed tech programs are best made transparently, with an opportunity for public discussion. All information about the programs and the reasons for adopting them should be communicated with parents. When agreements are made behind closed doors, they often backfire — badly. An oft-cited "cautionary tale" was the decision by education officials to pilot inBloom, Inc., the $100 million project of the Gates Foundation. Nine states and districts agreed to share personal student information with this corporation, without any public discussion of the goals or the need for such disclosure. The project collapsed after parent backlash. Educators would be wise to learn from this colossal blunder and include all stakeholders, including parents, teachers, and the students themselves, before making decisions to hand over their personal data to private hands.

Outside influence or compensation

In fall 2017, the *New York Times* reported on Silicon Valley's untoward influence over certain educators responsible for adopting ed tech. In some cases, school officials were accepting compensation or travel expenses paid for by vendors in return for acquiring their digital products. The former superintendent of Baltimore County Public Schools was indicted, in part, for failing to disclose payments he received from a firm that arranged meetings between himself and ed tech companies seeking contracts with his district.

The practice of companies offering perks or other compensation to public officials isn't just unethical; in at least two states, it's explicitly illegal. Delaware and Maine have passed legislation barring teachers and administrators from recommending the use of online educational materials, content, services, or other products if they received any compensation for "developing, enabling, or communicating such recommendations." Whenever implementation of ed tech is proposed, make certain that the person bringing forward the idea or involved in the decision will not personally benefit as a result.

Survey Results:

Our survey found that 7 percent of educators had been offered compensation by a vendor to use, assign, promote, or evaluate an ed tech program or device. Of those educators, 17 percent had agreed to use the app in exchange for money. When asked if their district or school barred teachers from receiving compensation from ed tech companies, 8 percent said yes, 10 percent said no, and the rest did not know or were unsure.

Authority to make the decision

Before adopting ed tech, educators should be working with their school district's legal counsel as well as Information Technology specialists to evaluate these products and their Terms of Service (TOS), Privacy Policies, contracts, or other written agreements to ensure compliance with federal and state law.

When schools or individual teachers are authorized to adopt ed tech programs and apps without oversight, they should exercise extreme caution. Federal law and many state laws require specific conditions to be met before personal student information can be shared with third parties without parental consent.
See Section III for more information.

Truthfully, no teacher should be enabling access to student data without proper legal guidance, especially if the product is free. Companies offering free products rarely, if ever, are doing so for philanthropic reasons. Rather, most are start-ups funded by venture capitalists looking for opportunities to monetize and profit from your data or the data of your students. And if you checked a box agreeing to the Terms of Service (TOS) and Privacy Policy before using it, often referred to as a "click-wrap" agreement, you are likely a party to a legally binding contract. Unless you are certain that the company's policies adhere to all applicable student privacy laws, it's best not to use it.

Survey Results:

When survey respondents were asked if they used education-related apps not required by the school or district, 74 percent said yes, 13 percent said no, and 13 percent said they didn't know.

Potential health effects

Physicians and other health experts have become increasingly concerned as schools assign their students to spend more time online. While official medical guidelines on appropriate screen time are in flux, many parents are also understandably worried that children spend many hours in front of screens — whether for entertainment or educational purposes — and that they may suffer physical and psychological harm as a result.

In a startling study recently released, researchers found that 1.1 million U.S. 8th, 10th, and 12th graders surveyed annually from 1991-2016 reported that their "psychological well-being (measured by self-esteem, life satisfaction, and happiness) suddenly decreased after 2012"— a time when smartphone technology and screen time use was on the rise. The study also reported that children who spent the least amount of time online, whether on social media, the internet, texting, or gaming, tended to be the happiest.

> "Gamification" is quickly becoming a popular trend in education. Marketed as a way to motivate and engage learners, students are spending increasing amounts of time in class and at home playing "educational" online video games. This is particularly problematic given the World Health Organization's classification of "gaming disorder" as a new mental health condition in June 2018.

In 2018, the Maryland legislature took a step towards acknowledging the risks to children of increasing screen time by mandating their state education department work with their state department of health to develop "health and safety best practices" related to ed tech use in schools. In the absence of adequate national guidelines, other states should follow Maryland's example to take this issue seriously.

> Advocacy organizations like the Campaign for a Commercial-Free Childhood (CCFC) are taking the lead to inform and engage the public about the known risks of increased screen time. In 2017, CCFC created the Children's Screen Time Action Network, a "coalition of practitioners, educators, and advocates working to promote a healthy childhood by reducing the amount of time kids spend with digital devices." The Network's website at www.screentimenetwork.org includes videos and other helpful resources for parents and educators who would like to learn more about the potential side effects of excessive screen time, including technology addiction, depression, obesity, and stress.

But increased screen time isn't an issue solely affecting adolescents. Teachers also are concerned about the impact to their own health and well-being from the increased use of technology in the classroom. The Badass Teachers Association and the American Federation of Teachers conducted two quality of life surveys of educators nationwide in 2015 and 2017. Many educators responding to these surveys expressed dissatisfaction with the overuse of tech in schools. One teacher reported that "non-stop dumping of new teaching strategies, data collection … [and] technology, etc. has sucked the joy out of teaching." Another teacher responded that "too much emphasis on students having technology … is more of a distraction than a support in many cases ..." Our own survey of educators received similar responses. For a summary, see Appendix B.

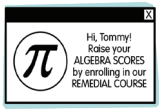
Financial cost

The cost to deploy some ed tech systems can skyrocket into the millions — not even accounting for costs associated with training, maintenance, and upgrades. These expenses can take a heavy toll on districts already struggling to maintain basic services. Before adopting large-scale ed tech programs, educators should ask questions about the short- and long-term expense of such programs and if the district is able to sustain these costs in the future.

This should also be the case with free ed tech. Sensing an opportunity to gain a competitive advantage, some companies offer schools devices or software at no cost in the form of "pilot" programs. Eager to accept the gifts, decision-makers may jump in before fully contemplating how the new technology will be funded in the future. Other companies permanently offer their services or apps for "free," in which case teachers and students are likely paying with their personal data.

Survey Results:

In response to our survey, 10 percent of teachers said they were aware that education-related apps that they use sell student data or use student data for marketing purposes.



Algorithms and "adaptive learning"

Some ed tech products touting "adaptive," "predictive," or "personalized" learning capabilities use "black box" algorithms, a term used to describe mathematical formulas that are so mysterious or complex that outsiders cannot examine or understand them. These algorithms use data to present material or ask questions to students based on their prior performance — or the performance of students who are believed to be similar to them, according to some measurable characteristic.

When black box algorithms are used to drive educational software — for example on the Smarter Balanced Assessment Consortium (SBAC) exams, the IXL online curriculum, or the Learning A-Z's Raz-Plus "personalized"

reading program — schools cannot validate their accuracy and ensure they don't have an inherent bias to discriminate against students based upon their race, gender, economic background, or other factors. If outcomes from these programs are attached to high-stakes consequences, such as grades, promotion, or teacher evaluations, students and teachers are unable to challenge the validity of the results because the algorithms are often treated as trade secrets that the company cannot be compelled to divulge. For this and other reasons, algorithms used in education are facing increased scrutiny.

One expert has recently called the use of algorithms "alchemy." Another, Larry Berger of the curriculum and assessment company Amplify, has expressed doubt that adaptive learning as currently designed works at all. New York City recently created a task force, said to be the first of its kind in the U.S., to examine algorithms used in governmental decision-making, including in the public schools. There is a growing consensus that algorithms should not replace the judgement of human educators, and any school considering adopting these products should use extreme caution and make certain no high-stakes decisions are attached to their use.

Uses of teacher and student data and their deletion

Ed tech vendors should be transparent about their data practices. Contracts and other written agreements should be made publicly available and explain clearly what specific data the vendor collects, the purpose for its collection, with whom the data will be shared, how it will be secured, and how the company will notify all users in cases of breach. The U.S. Department of Education's Privacy Technical Assistance Center offers resources to schools in this area, including a section of its website dedicated to security best practices. If you're unable to find straightforward information about a vendor's data practices, the company may be doing something that it shouldn't.

> Researchers at UC Berkeley's International Computer Science Institute (ICSI) published an analysis of children's apps and found that the majority fail to provide adequate protections to prevent misuse of user data. They developed a privacy analysis tool (http://AppCensus.mobi) that provides detailed information about the kinds of personal information accessible to vendors from using the Android versions of over 76,000 apps, including many employed in the classroom. For example, the ICSI evaluation of the ClassDojo app, a popular classroom tool used to track student behavior, revealed that it uses and transmits "sensitive information."

Contracts with ed tech vendors should also acknowledge that the district controls all the data it collects and maintains on behalf of the school, and that the vendor will return and delete it upon request or when the contract expires. In cases where teachers are permitted to sign up for classroom apps, they must ensure that the Terms of Service (TOS) state clearly that the school (or teacher) is in control of the data and can have it destroyed at the end of the school year. (Note: This is good practice, and you should be sure to demand this annually as well.) Teachers should look to see if the TOS claims royalty-free license to use, copy, reproduce, adapt, publish, or distribute content uploaded by teachers and students without explicit permission or compensation — which would imply that the data is really not under your control. Vendors may also claim the right to use the data to develop and improve their products and services. Both these claims could run afoul of FERPA, as described on page 25.

Parental permission

In some cases federal law requires schools to obtain consent before disclosing student information to third parties. The U.S. Department of Education suggests that "even in instances where FERPA [Family Educational Rights and Privacy Act] does not require parental consent, schools and districts should consider whether consent is appropriate." It's best to err on the side of caution and ask parent permission whenever possible prior to sharing their children's information with vendors or organizations.

Moreover, schools cannot coerce parents to consent to the Terms of Service (TOS) of online programs if the companies allow for data sharing with third parties without restriction. In November 2017, the Department determined that Agora, a Pennsylvania cyber charter school, violated FERPA by forcing parents to accept the TOS of K12 Inc., the online platform used by the school, as a condition of enrollment. The TOS gave K12 Inc. and its affiliates and licensees "the right to use, reproduce, display, perform, adapt, modify, distribute, have distributed, and promote the content in any form, anywhere and for any purpose," including personal student information. This finding should send a strong message to schools: ensure that your ed tech vendors don't use student data for purposes not authorized in FERPA, and if they do, it's your legal obligation to obtain explicit, voluntary parental consent.

SECTION V:
Limit social media use in school with ten simple rules to follow

A growing body of evidence suggests that the use of social media can be harmful to the mental health of both adults and children. Some studies have found it to be addictive and stressful, and it can even contribute to jealousy and loneliness. Its use can also allow schools and districts to monitor the private lives of teachers and students, either overtly or surreptitiously.

Despite these warnings, many teachers and schools commonly employ social networks, like Facebook, Instagram (owned by Facebook), YouTube (owned by Google), Twitter, and SnapChat, to communicate with students and their families, to promote school-related clubs and activities, or for instruction.

Schools with official accounts or policies that require teachers to use social media for education-related purposes should reconsider these practices for reasons explained below. We urge teachers to refrain from choosing to communicate with their students or their families through social media or to assign students to use it as part of their lesson plans. Those who do so anyway should take special care to protect their professional reputation and privacy and that of their students. We provide some helpful tips on how to manage this at the end of this section.

Why you should say "No" to school-sanctioned social media

When schools rely on social networks and platforms like Facebook to communicate with families, students and parents may be forced to create accounts to access important updates. Equity issues arise for families with limited access to the internet. Other families may be coerced to use these platforms against their will. Additionally, young students may be unable to access school content on social media networks because most platforms legally prohibit children under the age of 13 from creating accounts without parental approval, in compliance with the Children's Online Privacy Protection Act or COPPA. For more on COPPA, see Section III.

In addition, a student's photo, name, school, and other personal information is protected by FERPA, the Family Educational Family Rights and Privacy Act. Publicly posting this information on social media without parental consent may violate this law in some circumstances — for example, if a parent has opted-out of directory information disclosure. For more on what FERPA requires, see Section III.

Even if allowed by law, some parents may have their own legitimate concerns about sharing their children's information online. If the thought of handing a photo of your students to a stranger on the street makes you uncomfortable, then you can understand why you should reconsider posting their photos online.

No educational value

Posting pictures on social media of students engaged in school activities or classroom projects may sound fun and exciting – especially as those "likes" roll in – but children attend school to receive an education, not to promote a school or teacher's online profile. If you can't justify the educational value of social media, then don't use it.

Big Brother is real

School districts are increasingly monitoring students' social media accounts for signs of depression, isolation, resentment, or bullying, either directly or with the help of third-party services. If students are required or pressured to engage with social media to access information they need for school, they may also be subjected to increased levels of surveillance by school districts, the state, corporations, or law enforcement. For example, some social media monitoring tools employed by police use geofence or virtual fence technology that track and capture any public posts made within a specified geographical area, usually around schools, sporting events, or other areas of interest. Posts can be used to identify and target potential suspects, sparking concerns from civil liberties advocates.

With the rapid rise of big data analytics that include controversial uses of artificial intelligence, machine learning, facial and voice recognition, and social-emotional analysis, students and teachers are at increasingly higher risks of having their behavior tagged with erroneous and damaging labels.

> Recent reports revealed that the New York City Police Department maintains a database of "suspected gang members" with more than 42,000 names, including more than 1,300 minors under the age of 18. Among the reasons individuals were placed on this list include staying out late and changes in behavior, as well as the use of video games, SnapChat, or Instagram.

> The surveillance of students' social media use is contributing to the school-to-prison pipeline, according to Community Solutions, a nonprofit organization that specializes in evidence-based programs to prevent excessive disciplinary practices. New laws have been passed in several states that require schools to refer students suspected of cyberbullying to law enforcement.

Survey Results:

Teachers are being tracked through their use of social media as well. In response to our survey, 12 percent of teachers responded that their district monitors their use of social media, with 10 percent reporting this happens even when they are not using the school's computer system.

Deceptive business practices

YouTube, considered by many to be a social networking site, is increasingly being used in schools to stream lecture content and to deliver tutorial videos. In spring 2018, twenty advocacy groups, including the Parent Coalition for Student Privacy, filed a complaint with the Federal Trade Commission (FTC) over YouTube's deceptive practice of collecting personal information, including geolocation, from children under the age 13 without parental consent, in violation of COPPA. YouTube ***claims*** that users must be at least 13 years or older to use the site, but as the complaint demonstrates, the platform ***actually*** contains a great deal of content aimed specifically at young children.

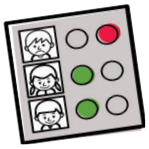
In June 2018, eight consumer advocacy groups filed an FTC complaint against Facebook and Google, describing the manipulative tactics these companies use to trick users into unknowingly giving their consent to allow them to collect and use their personal data for commercial purposes. We must remain vigilant to the deceptive practices of all social media outlets, no matter how fun they may be.

When "free" isn't free

The manner in which the "free" business model of Facebook, Google, and other social network companies make a profit is to capture as much behavioral and other online information from their users as possible in order to build consumer profiles and then charge companies who want to serve ads based upon these profiles.

Even if a social media platform doesn't collect user information for these purposes, online advertising companies or "ad tech" does. This means that regardless of the social network's own policies, advertising companies like DoubleClick (a subsidiary of Google) are capturing data, such as the time spent on a webpage and the links clicked, to serve ads connected to the user's interests.

Moreover, social networks are known to have long, confusing, and ever-changing Terms of Service and Privacy Policies, describing how their corporate partners, service providers, and other third parties are acquiring and treating user data. It's difficult, if not impossible, for the average person to wade through these complex documents to know exactly how their online information will be data-mined, shared, or sold by a social network on any given day. Students and their families should not be required to use social media platforms that can share, sell, and use their data for advertising, marketing, or other commercial purposes.



The "creep" factor

Facebook's CEO Mark Zuckerberg ignited global controversy following his congressional testimony in the spring of 2018 over the social network's plans to perfect its facial recognition technology. The software analyzes photos and videos of its 2.2 billion users for unique physical characteristics, creates "templates," and then scans and analyzes every photo uploaded to suggest friends for users to tag. This can pose serious dangers to students' physical safety, particularly in instances of child custody disputes. Additionally, states such as Texas, Washington, and Illinois have recently passed privacy laws limiting the biometric data that companies like Facebook can collect from its users, including photos. To avoid these risks, it's best to refrain from posting any pictures of your students to social media, and you should encourage your students not to post pictures of themselves or their classmates either.

Ten tips for teachers using social media for personal use

Teachers should take extra steps to protect their personal data, public image, and professional reputation. If you elect to use social media for personal reasons, make sure you know how to use it safely. Here are ten simple rules to follow:

1. **GET TO KNOW** your school or district policies and state laws on personal social media use.

2. **REGARDLESS** of which social media platform you use, set your account to "private" and select the strongest privacy settings possible. Check the platform's online help centers to walk you through the process.

3. **DON'T ASSUME** everything you post will remain private, even if you maximize the privacy settings. As recently as June 2018, a Facebook software "bug" publicly exposed the posts of over 14 million users. For any sensitive information you share, you must presume that it may someday become public.

4. **NEVER** include your school name or affiliation on your profile.

5. **DO NOT** "friend" or "follow" students on social media, and be clear with your students not to friend or follow you. As a preventive measure, be sure to block any student who has sent you a friend request on Facebook or SnapChat or who has attempted to follow you on Twitter or Instagram.

6. **BE CAREFUL** when posting any negative comments concerning your school or district. While the First Amendment protects free speech, it becomes complicated when the speech relates to one's official duties, especially when criticizing your employer. If you do post something critical, consider including a disclaimer noting that your comments reflect your personal opinions and not those of your employer.

7. **NEVER** post any pictures or other identifying information about your students. This may be a violation of FERPA, as mentioned previously. If you choose to post a narrative about your students — positive or negative — it could put you in jeopardy of losing your job or facing other disciplinary actions.

8. **KEEP** your profile pictures free of alcohol, drugs, or anything else that could be interpreted as controversial or offensive. Even if you lock down your Facebook profile for privacy, it can still appear on search engines unless you turn them off. Also, when Instagram users with private profiles share photos or videos to Twitter or Facebook, the image may be visible to users on that platform and publicly accessible to anyone with a direct link.

9. **BE MINDFUL** of what you "like" and "favorite" on social media. Fairly or not, you are likely to be judged accordingly. Even if unintended, your likes may be interpreted as an endorsement.

10. **TO AVOID** public scrutiny, don't post during the school day, when you are supposed to be at work.

SECTION VI:
Best practices and practical tips to protect teacher and student privacy

Do your homework

- **BECOME FAMILIAR** with relevant federal and state employment and social media laws. You should also know your school, district, or other policies concerning your privacy.
- **INVESTIGATE** which personal information your school, district, and state are collecting about you and your students and how the data is being used. Arm yourself with this knowledge so you can make informed decisions about the data you share. To learn how teacher and student data are at risk, see Sections I and II.
- **CAREFULLY READ** the Privacy Policy or Terms of Service (TOS) of any app or program used in your classroom to determine whether it complies with state and federal privacy law. The U.S. Department of Education provides guidance to help educators evaluate common terms found in TOS, including examples of "red flags" to avoid. See the Resources section for a link to this guidance. You can also ask your administrators for a copy of the contract or service agreement with a vendor. The Massachusetts Student Privacy Alliance provides a model agreement you can compare it with. Find the link in the Resources section.

> Some ed tech vendors may claim rights to your and your students' intellectual property in their TOS. For example, the TOS of the free coding website Code.org grants the organization "a worldwide, non-exclusive, transferable, assignable, fully paid-up, royalty-free, perpetual, irrevocable right and license to host, transfer, display, perform, reproduce, modify, distribute and redistribute, adapt, prepare derivative works of, use, make, have made, import, and otherwise exploit" computer code or other materials that students post or upload to the program.

Resist the urge

Ed tech companies often exploit teachers and administrators by recruiting them to use and recommend their products in exchange for compensation, such as travel expenses to conferences or free devices. Acting as an "ambassador" in promoting a product and receiving any sort of compensation is ethically questionable and can run afoul of district policies or state laws. See Section III for more details.

- **IF YOU HAVE A CHOICE,** don't use social media for school-related purposes. If your school requires you to use a social network, discuss this with your union and the administration. If you choose to use it anyway, learn about how to protect your students' privacy, as well as your own. Section V explains how.
- **DO NOT USE** any apps or online programs that have not been vetted by your district technology officer, and whenever possible, ask for parental consent beforehand.

- **IF TEACHERS ARE AUTHORIZED** to adopt tools on their own, resist the urge to use "free" apps with "click-wrap" agreements that just require checking a box to accept the TOS. This action can make you party to a legally-binding contract whose terms may violate federal or state law. Moreover, you may unknowingly be paying with your students' data or your own.
- **IF YOUR STUDENTS** are under the age of 13, additional legal restrictions apply under COPPA — see Section III for more.
- **AT THE END** of the school year, make certain that you or school administrators contact each vendor to close any accounts and delete teacher and student data.
- **WHEN USING ED TECH,** ensure that the least personal information necessary for its operation is provided to the vendor. For example, if the use of an app isn't dependent upon uploading your photo or photos of your students, resist the urge to do so. If the app asks if a student has a disability or receives accommodations, don't offer this information unless mandated by your school or district.
- **IF YOU GIVE** surveys to your students, check to see if the questions touch on any sensitive areas as described in Section III under the Protection of Pupil Rights Amendment (PPRA). If they do, you must notify parents in advance and allow them an opportunity to consent or opt their child out of the survey.

Survey Results:

In response to our survey, an astonishing 44 percent of respondents said they did not know what happened to student and teacher data after the use of an app was discontinued; 37 percent reported no consistent policy was in place to address deletion of apps or data; and 12 percent said no one in their district acts to ensure teacher and student data are deleted when the app is discontinued. Only 7 percent of teachers said they or district administrators ask companies to delete teacher and student accounts after the app or program is no longer used.

Practice discretion

- **DON'T ATTEMPT** to access data for which you're not authorized, including students' attendance, grades, course schedules, and health information stored in digital information systems, such as Infinite Campus and PowerSchool. Federal law, including the Family Educational Rights and Privacy Act or FERPA, limits your access to only the information of those students for which you are directly responsible, and for purposes required to fulfill your professional responsibilities. See Section III for more detail.
- **WHEN ENTERING** your students' personal information into data systems, take extra precautions to ensure its accuracy. Student records can follow students for life and may be used for high-stakes decisions. To see how student data is at risk, see Section II.
- **BE CAREFUL** about accessing your students' previous grades or behavior information, which may lead you to lower your expectations or cause you to unconsciously prejudge them even before you've gotten to know them personally.
- **DATA WALLS** can do more harm to students than good. In addition to possible FERPA violations (see Section III), publicizing student rankings or performance can hurt student morale and undermine their motivation.

- **IF YOU ARE PROVIDED** with a device by your school, software may be preloaded that allows the district or school officials to monitor your movements or communications. The same is true of your school email account and/or your use of social media. Be mindful that you may be surveilled; be cautious when posting about your school, students, or administrators; and make sure that you use district devices and your official email account in a responsible manner.
- **IF YOUR SCHOOL** employs Google products, including Chromebooks and/or G Suite for Education with accounts for Gmail, Google Docs and other tools, the Electronic Frontier Foundation provides helpful guidance on how to set the defaults to minimize the data collected about you and your students. For links to their advice, see the Resources section.
- **CONSIDER** using a password manager or other secure method to store your login and passwords, and be certain to shred any scrap pieces of paper with this information that may be in view in your work area. And never share your passwords with anyone — including substitute teachers or student helpers. If you do so in an emergency, be sure to change them as soon as possible.
- **COVER YOUR LAPTOP** webcams with a sticky note or Band-Aid. After all, former FBI director James Comey and Facebook CEO Mark Zuckerberg do this.

Get involved

- **ENCOURAGE YOUR SCHOOL** or district to foster a privacy-conscious culture. Share this toolkit with your district office or, if applicable, your union leadership. Advocate for the creation of a school privacy oversight committee, including parents, teachers, students, and technical experts to give input on how to strengthen data privacy and security policies.
- **URGE YOUR DISTRICT**, school, and union to offer training and professional development on how to best protect student and teacher privacy.
- **IF YOU BELIEVE** your data privacy has been violated, or that of your students, raise your voice. Chances are you aren't the only one with concerns. Contact your local, state, and national unions for guidance, and see Section VII to learn how to advocate for stronger privacy protections.

SECTION VII:
How to advocate for stronger teacher and student privacy protections

After you've read about the serious risks associated with the increasing collection and disclosure of personal data, you may want to advocate for stronger privacy practices and policies to be adopted by your school, district, or state. Remember: educators are the guardians at the schoolhouse door. Teachers should engage and encourage responsible data use and the thoughtful implementation of technology. If you feel your school or district prevents you or your colleagues from doing so, here are some tips to help you advocate for better privacy protections.

Share this toolkit with others

We've tried to make this resource easy to share. Send the entire toolkit to your friends and colleagues as an email attachment or website link. You can also print a copy and leave it in the teachers' lounge or the library for others to flip through.

Please also suggest that your principal, superintendent, or union invite someone from our team to come and offer a professional development workshop on privacy and how to use the toolkit. To arrange this, please email us at *TeacherPrivacy2018@gmail.com*.

Find allies

Advocacy can be lonely and difficult unless others stand with you. Find other individuals who share your interest in this issue, whether they're colleagues, parents, union representatives, or members of advocacy groups. Exchange contact information and meet for coffee. There's no reason you can't enjoy yourself while also advocating for important causes.

You can also reach out to national organizations concerned with student privacy issues, including our organizations, the **Badass Teachers Association** at ***www.badassteacher.org*** or the **Parent Coalition for Student Privacy** at ***www.studentprivacymatters.org.*** Other groups that advocate on privacy include:

- **American Civil Liberties Union** — *www.aclu.org*
- **Campaign for a Commercial-Free Childhood** — *www.commercialfreechildhood.org*
- **Electronic Frontier Foundation** — *www.eff.org*
- **Electronic Privacy Information Center** — *www.epic.org*
- **Network for Public Education** — *www.networkforpubliceducation.org*
- **Privacy International** — *www.privacyinternational.org*
- **Student Data Privacy Consortium** — *www.privacy.a4l.org*
- **World Privacy Forum** — *www.worldprivacyforum.org*

You should also contact your local and state unions and their national organizations, whether the American Federation of Teachers or the National Education Association, who helped fund this toolkit.

Bring forward your concerns to school or district leadership

It's important to raise concerns about data privacy, especially as there are so many organizations and funders urging schools to expand the use of ed tech. If you're worried by any of the products being used at your school, ask administrators for a copy of the contract or service agreement with the vendor. The Massachusetts Student Privacy Alliance provides a model agreement you can compare it with. The Resources section of this toolkit contains more information. Remember, it is your right to access the contract or the product's Terms of Service under most states' Freedom of Information laws. Rely on your allies for support and request a meeting with school or district leaders to address your concerns. If you are told they will "get back to you," ask for a timeline and follow up promptly to keep the topic front and center.

Encourage your school or district to convene an oversight committee

If you believe your school or district could be doing better to protect teacher and student privacy — and everyone could be doing better — suggest that your school or district create a privacy committee or working group to provide guidance in this area. Parents and high school students should be included, as well as individuals with relevant professional experience in technology or cybersecurity.

Request that your local union adopt contract language to protect teacher and student privacy

If you are in a state that allows collective bargaining, local teacher unions can negotiate stronger privacy protections in their contracts. Share this toolkit with your building union representative who can bring the issue to your executive body for discussion. See Appendix A for sample contract language.

Ask your state union to develop resolutions or new business items to protect teacher and student privacy

If you believe that your state or national union should develop policies around teacher or student privacy, make an appointment with your NEA/AFT delegates — usually members of your executive body — to discuss creating a resolution or a new business item (usually referenced as an NBI) to be considered and voted upon at the NEA Representative Assembly or AFT Convention. You can do this on the state level in the same manner. Please see your local union president for guidance.

APPENDIX A:
Sample teacher contract language protecting educator privacy

Article V - Conditions of Employment

Section 5 - Protection of Personal Data

The district shall not require teachers to enroll in digital systems that transfer a teacher's right to his or her intellectual property to a private corporation, nor will the district sell or license a teacher's personal information to any third party for any reason or make it available for marketing or commercial purposes.

The district shall not disclose teachers' personal information to third parties without prior notification, and shall provide individual teachers with the right to opt out of disclosures for any purpose other than that which is required by the state for reporting purposes. Prior to the disclosure of teacher information to third parties for research purposes, teacher data must be fully de-identified and the study must have Institutional Review Board (IRB) approval.

The district shall provide annual training to all staff on the protection of teacher and student data, federal and state privacy laws, and best practices for protection of education-related data.

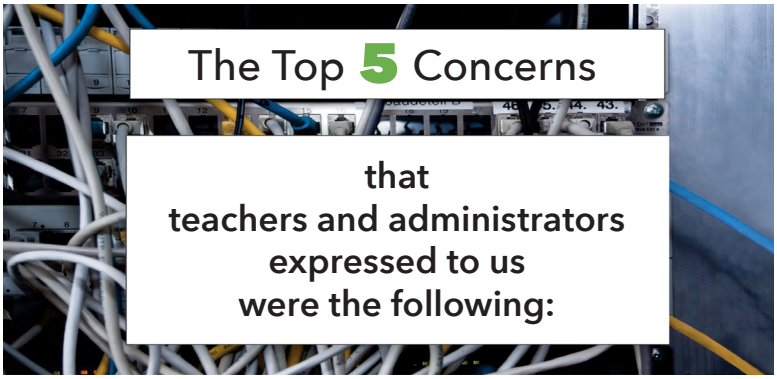
APPENDIX B:
Results from our educator survey, focus groups, and interviews on data privacy

In preparation for developing this teacher toolkit, the Badass Teachers Association and the Parent Coalition for Privacy conducted an online survey for two weeks, from March 4 to March 18, 2018.

We elicited responses from 365 educators from 45 states and the District of Columbia. The survey was promoted through Facebook, Twitter, and the newsletters of the BATs and the American Federation of Teachers. The survey questions can be found here: *www.bit.ly/BATs_PCSPsurvey*

About 86 percent of the respondents were classroom teachers; the rest were librarians and media specialists, assistant principals, instructional coaches, counselors, and speech and language pathologists. To acquire more in-depth understanding, we also conducted several interviews and focus groups online with both teachers and administrators.

What we found was that educators need support and training on how to protect both student data and their own, and they felt they needed to learn more about federal and state privacy laws.



1. **Too much personal data is being collected and shared with vendors, with the risk that it may be monetized.**
2. **Educators are being forced to implement ed tech products, which use data in ways they do not understand.**
3. **There is a critical need for more training on how to protect their own personal privacy and that of their students.**
4. **They want to learn more about what state and federal student privacy laws require.**
5. **They are worried that as the use of ed tech grows in the classroom, human interaction and individualism are being undermined.**

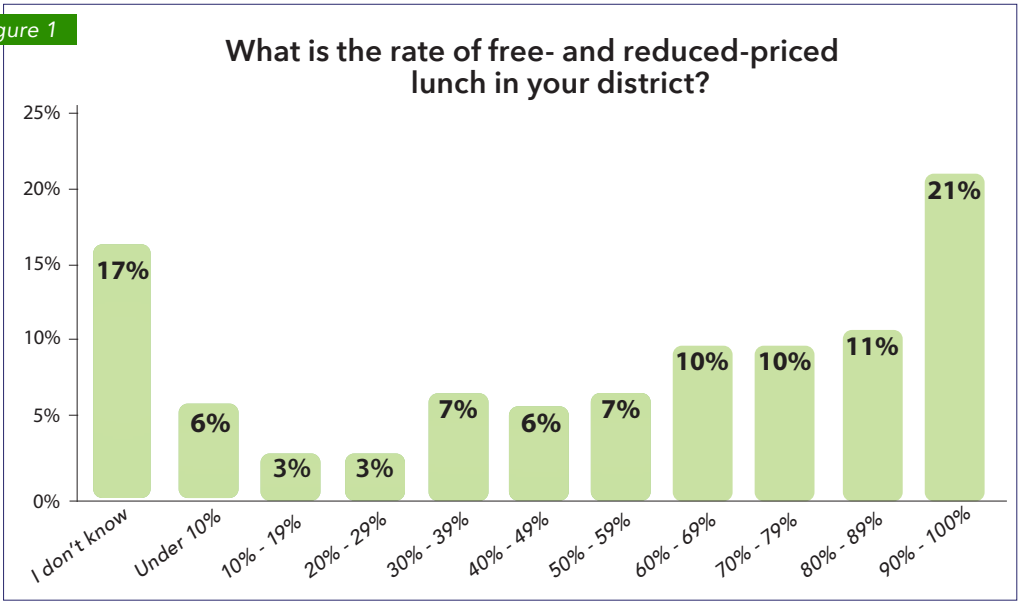
I. Online survey

Demographic background of respondents

Of the 365 respondents, nine percent worked in Pre-K and Kindergarten, 35 percent worked with middle school students (grades 6-8), 40 percent worked with high school students (grades 9-12), 4 percent worked with postsecondary students, and 50 percent worked with elementary students (grades 1-5). The responses indicate that some of the educators worked with students in multiple grade levels.

A large majority taught in urban areas (44 percent), followed by suburban (37 percent) and rural school districts (14 percent). When asked about their districts' poverty level, 21 percent of respondents reported an average free and reduced lunch rate of 90-100 percent. Seventeen percent didn't know. *(Figure 1)*

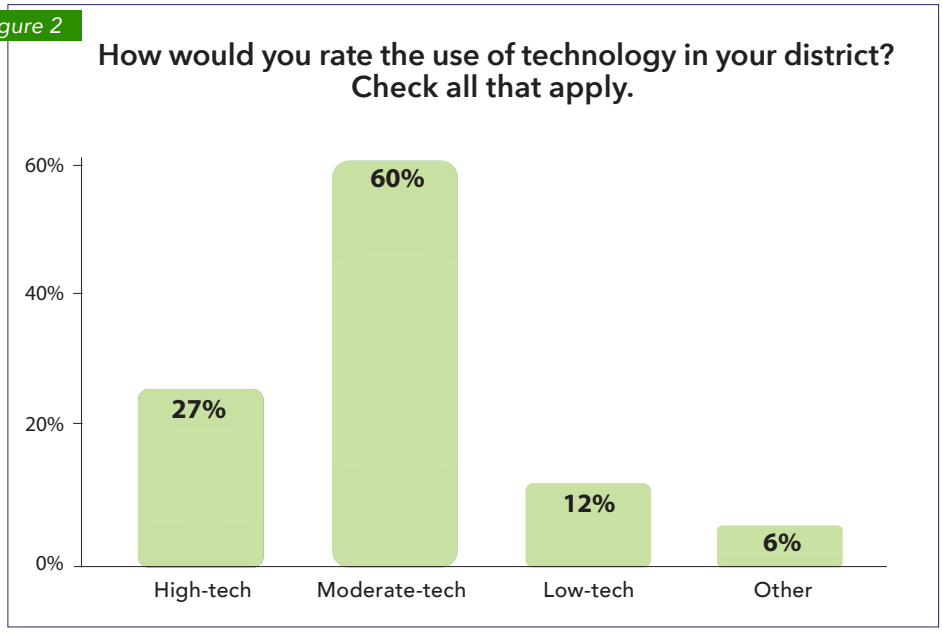
Figure 1



Technology use is widespread

Most educators (60 percent) reported their district used a "moderate" amount of technology; 27 percent said their districts used a high amount and 12 percent low. *(Figure 2)*

Figure 2



High use of technology was defined as the district supplying devices to each student or requiring they bring their own, as well as the use of digital textbooks. Moderate-tech was defined as making laptops widely available on demand, with some online course or material required and classroom apps encouraged. Low-tech meant the use of devices was limited to computer labs or the library, with a minimal assignment of online courses or instruction.

Many teachers reported that despite their high to moderate use of technology, they did not have any professional development or training in data privacy. "I know very little, I don't even know what I don't know," a teacher said.

Many also expressed a need for user-friendly materials on the subject that would be understandable to their colleagues, parents, and the community. One noted: "Always a concern, as it is in our private lives. We are all over Google Classroom and Chromebooks and I don't know what legal guarantees we have from them to not use or sell student use information."

In general, many teachers felt overwhelmed with the use of technology that is demanded of them. In many cases, teachers are now rated on how much they use digital apps. One responded, "Data data data !! The administration has become so bogged down in this idea of data-driven teaching that the teachers don't have time to create engaging learning activities."

When asked if their district used online programs to track student behavior, nearly half (48 percent) said yes, 43 percent said no, and nine percent didn't know. Twelve percent said their districts used online programs for social-emotional learning, while 62 percent said they did not, and 26 percent didn't know. *(Figures 3 and 4)*

Figure 3

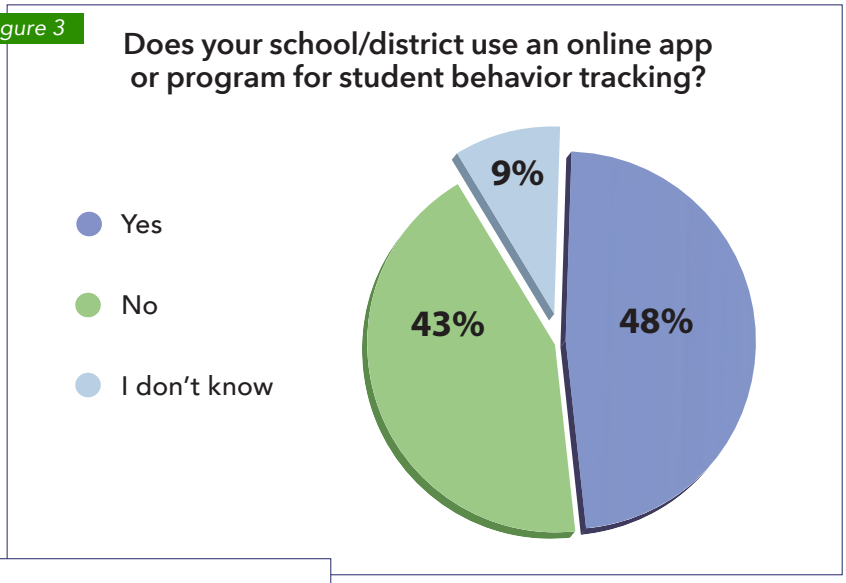
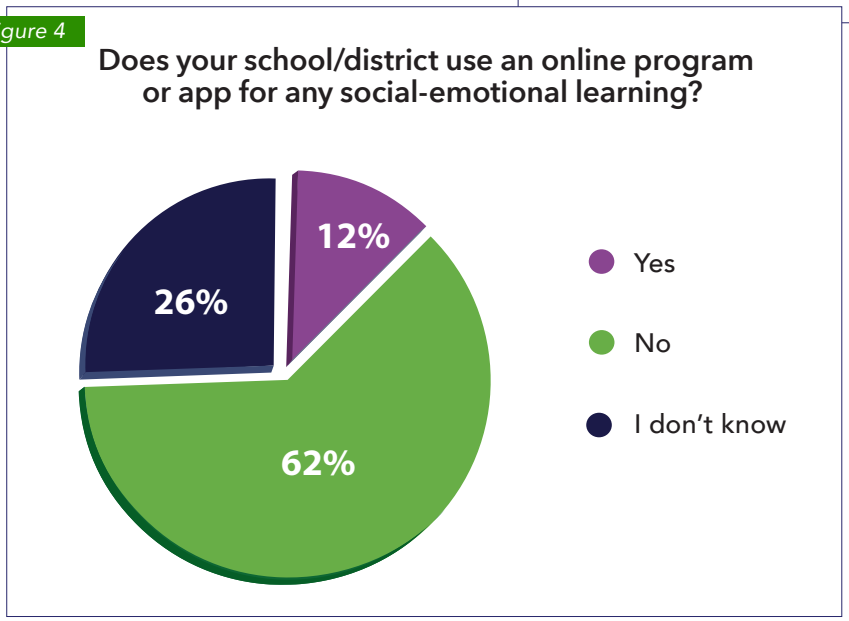


Figure 4

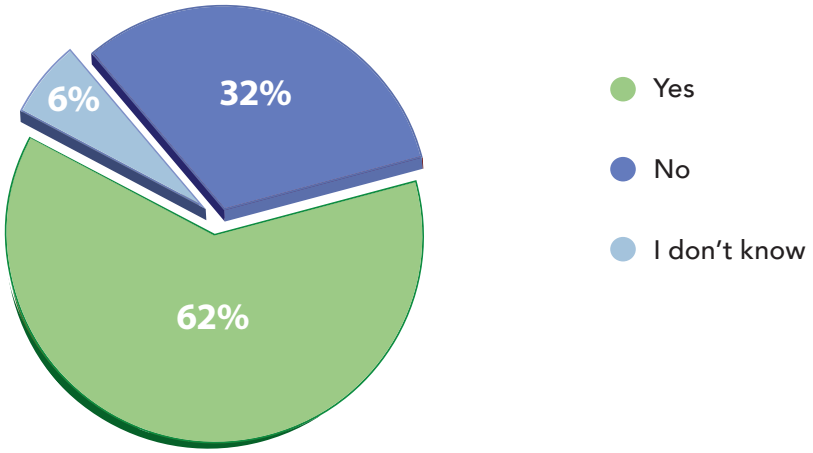


Who makes the decision to use online programs and/or evaluates them?

When we inquired if their school or district required teachers to use or assign students to use education-related programs, 62 percent of respondents said yes, 32 percent said no, and six percent didn't know. *(Figure 5)*

Figure 5

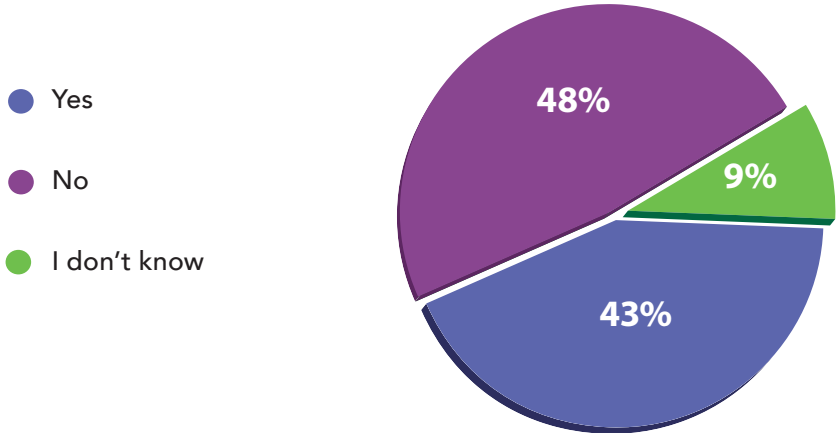
Many districts and schools assign students to use online instructional and assessment programs loaded onto computers. Does your school or district REQUIRE teachers to use or assign students to use these types of education-related programs?



We asked respondents if their schools or districts asked them to use apps with click-wrap agreements. (Click-wrap agreements are those for which a teacher, student, and/or parent creates a separate account for each student and then clicks on an "I Accept" button, thus agreeing to the company's Terms of Service or TOS. Most of these apps are free — though some may monetize student data in ways not made clear in the TOS.) Again, nearly half (43 percent) of our survey respondents said yes, their schools or districts require the use of ed tech with click-wrap agreements; 48 percent said no, and nine percent didn't know. *(Figure 6)*

Figure 6

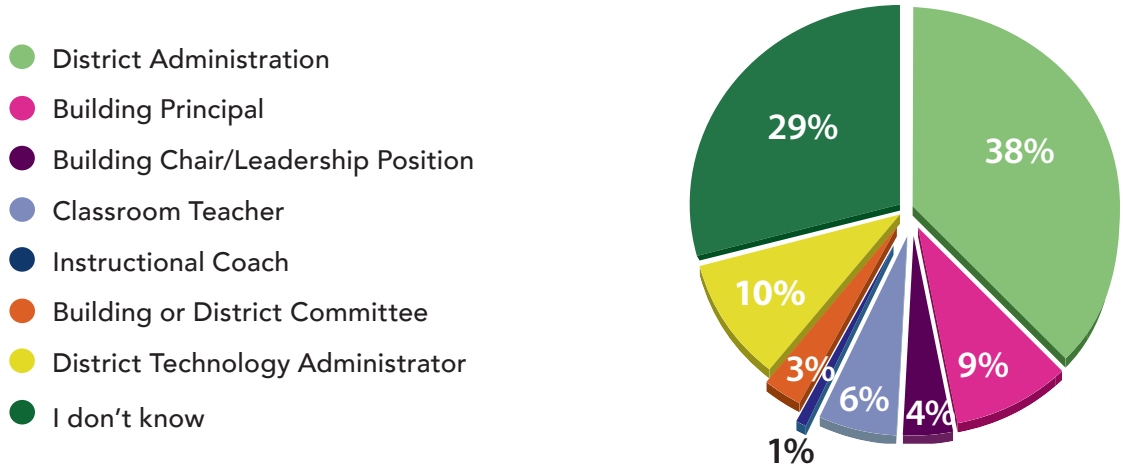
Does your school or district REQUIRE teachers to use these types of education-related apps (click-wrap agreements)?



Thirty-eight percent said district administrators made decisions about the use of education related apps, six percent said classroom teachers, and 29 percent didn't know who made these decisions. *(Figure 7)*

Figure 7

If your district or school REQUIRES the use of education-related apps, who makes the decision to use them?



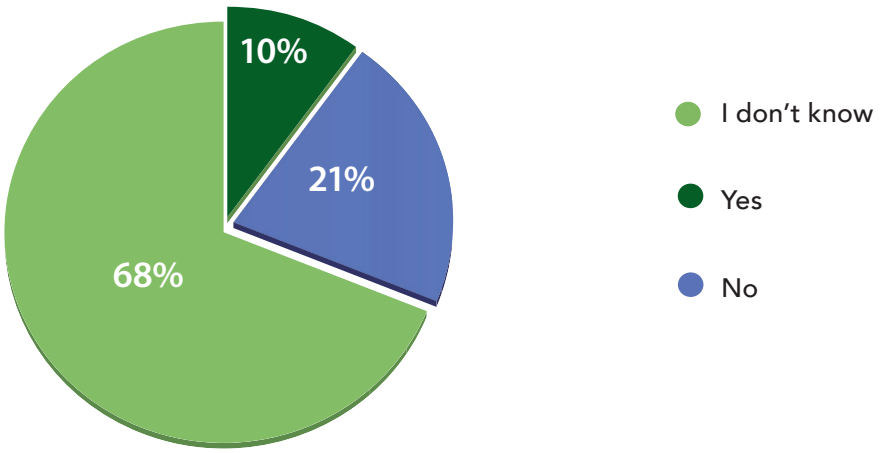
We asked how teachers learned about any education-related app or program that was not required by the district; 56 percent of respondents said they learned about it from a colleague, 48 percent said at a professional development/ faculty meeting, and 41 percent said at an education conference.

Lack of knowledge about how these apps use, delete, or sell student data

Given the widespread use of educational apps and programs, one of the most concerning results was that a large majority (68 percent) of our respondents didn't know if the vendors of these programs sold student data or used it for marketing or commercial purposes. Of the rest, 10 percent said yes, and 21 percent said no. *(Figure 8)*

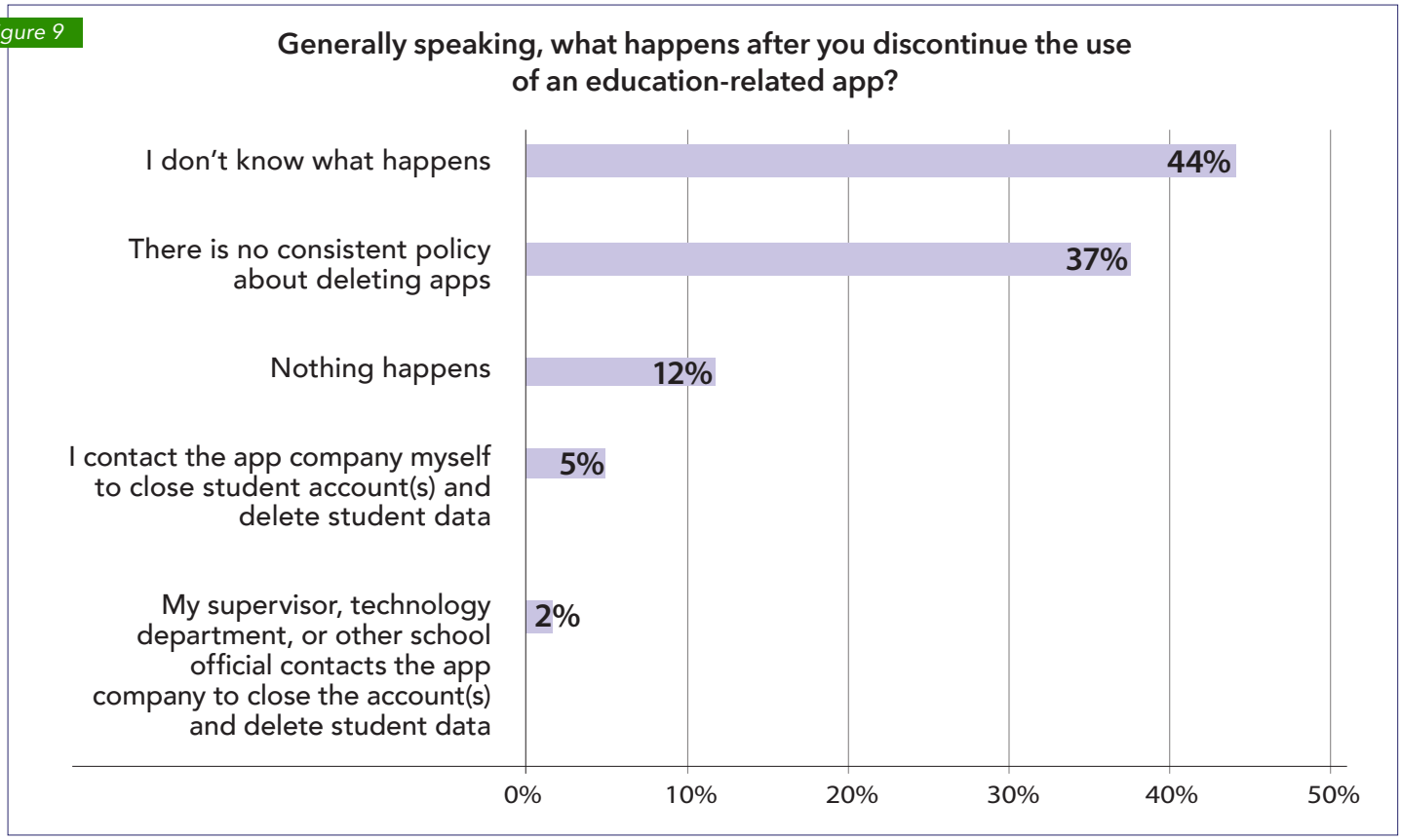
Figure 8

Do you know whether any of the education-related apps you use or assign sell student data or use student data for marketing or other commercial purposes?



When asked if the school or district demanded that the vendor delete the student data after the use of a particular app was discontinued, 44 percent said they did not know, 37 percent said there was no consistent policy, and 12 percent said nothing happened. *(Figure 9)*

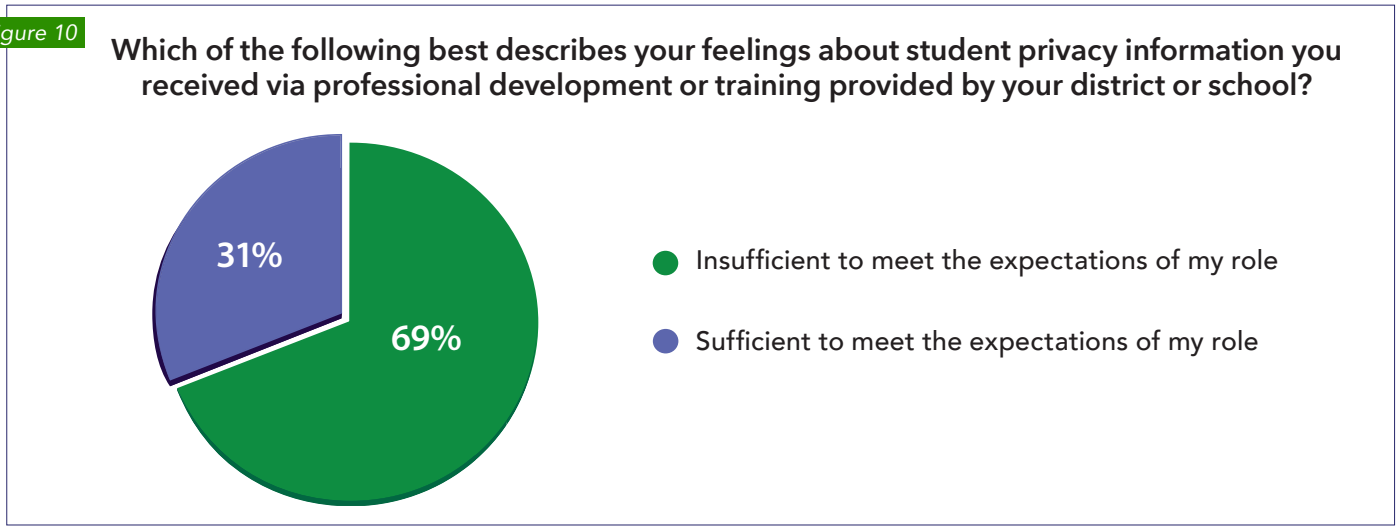
Figure 9



Lack of familiarity with federal and state privacy laws

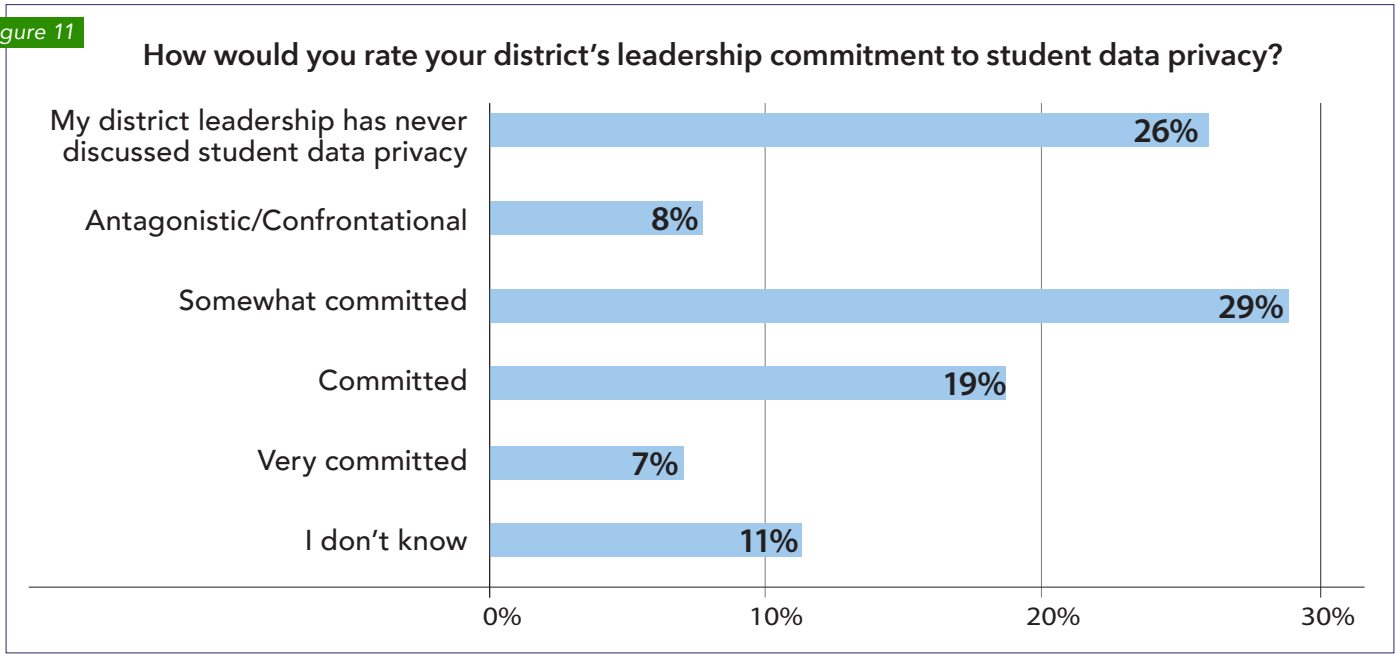
In preparing this toolkit, we wanted to find out how much educators already knew about student or teacher data privacy. A large majority of survey respondents (69 percent) said that the data privacy training they got from their district or school was insufficient. *(Figure 10)*

Figure 10



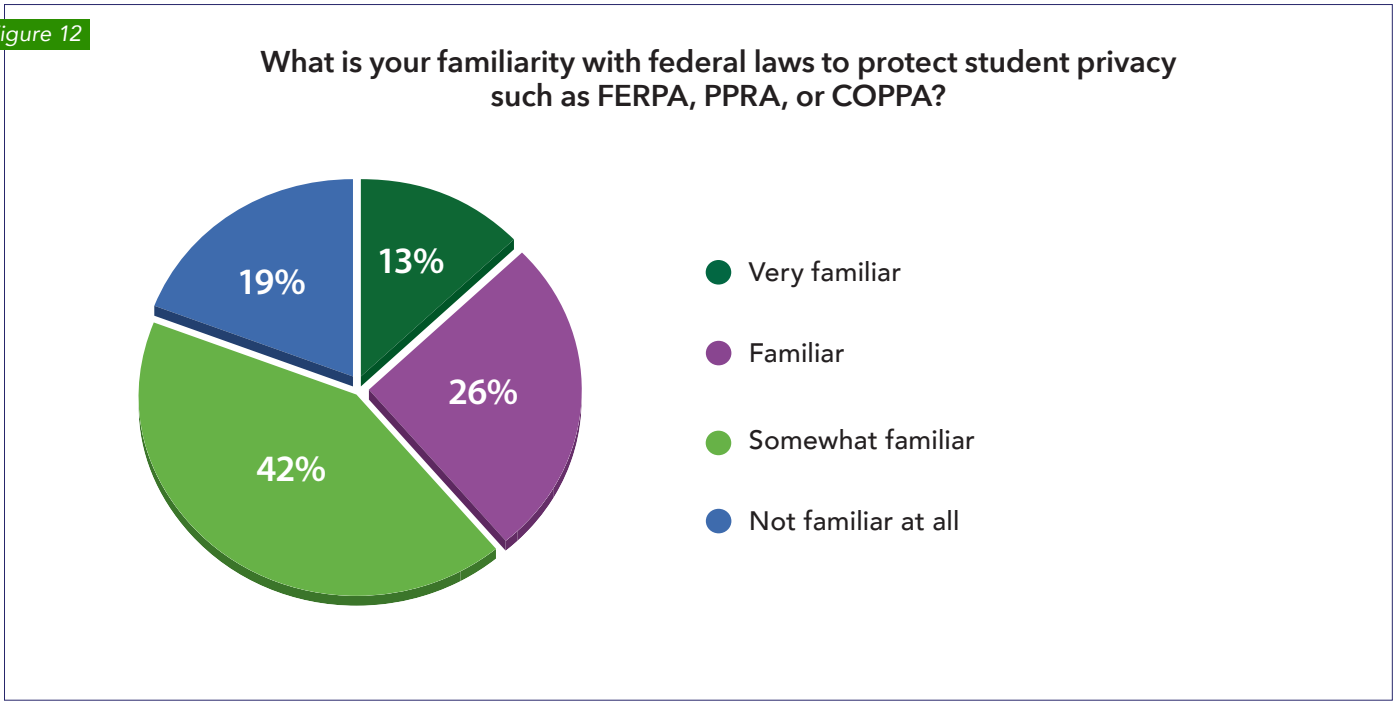
When asked about their districts' commitment to student privacy, 29 percent felt their district was somewhat committed, 26 percent reported that their districts were committed or very committed to student privacy, and 26 percent reported their district had never discussed the issue at all. Eight percent said that their district was antagonistic toward the issue. *(Figure 11)*

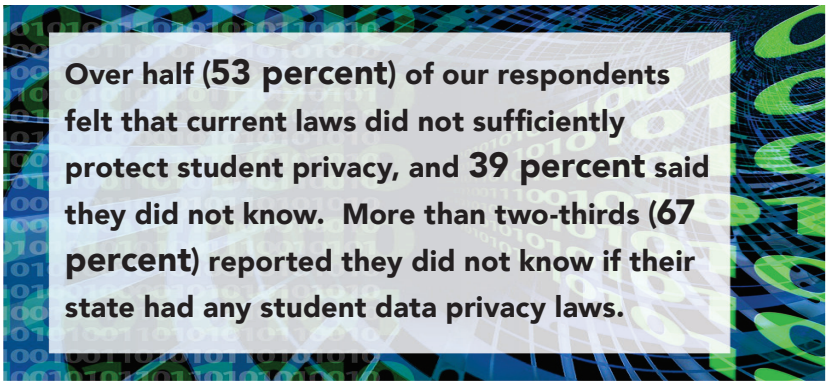
Figure 11



When asked if they were familiar with federal laws to protect student privacy, including **FERPA** (Family Educational Rights and Privacy Act), **PPRA** (Protection of Pupil Rights Amendment), or **COPPA** (Children's Online Privacy Protection Act), 13 percent said they were very familiar, 26 percent said they were familiar, 42 percent said they were somewhat familiar, and 19 percent said they were not familiar at all. *(Figure 12)*

Figure 12





Nearly a third (30 percent) of participants said that they learned about federal student privacy laws from their school district; 23 percent said they learned about it from the news and other reading, and nine percent said they learned about it from their union.

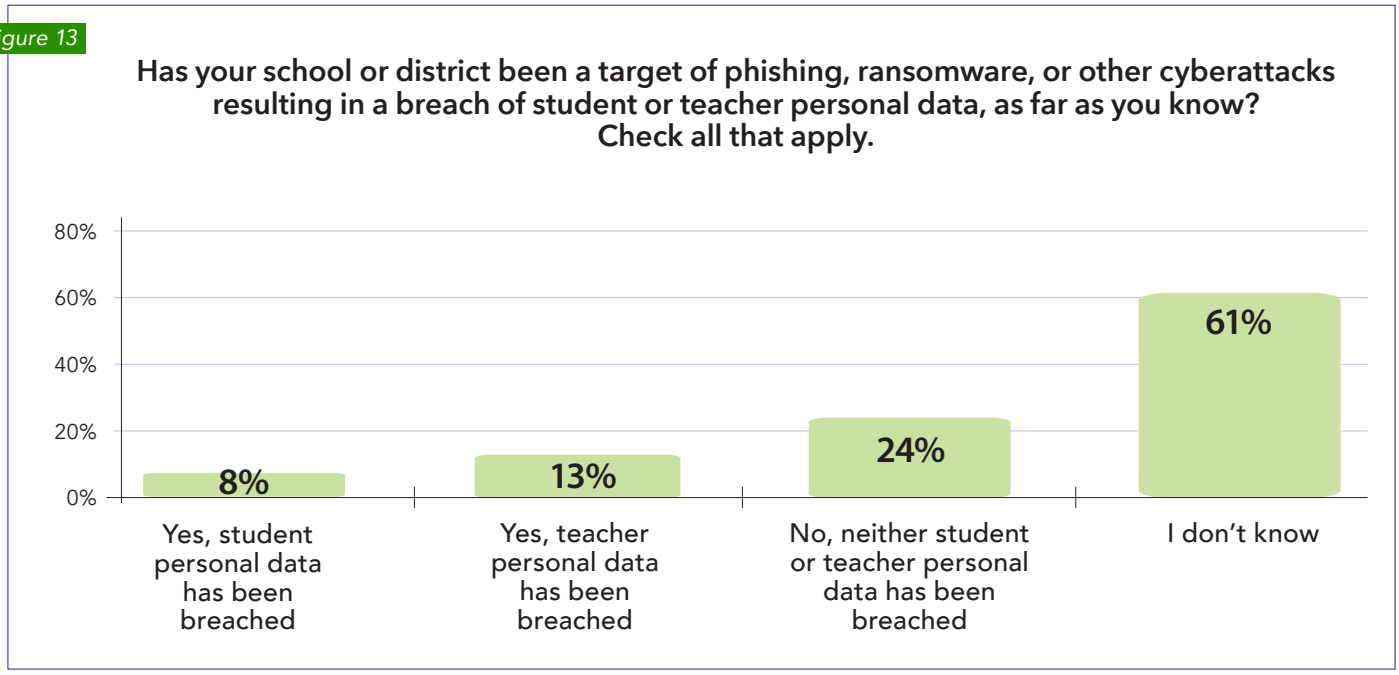
Use of student information systems

Nearly all (91 percent) of the participants reported that their district uses student information systems or data dashboards to track students' grades, attendance, enrollment, and other progress over time (for example, Infinite Campus, PowerSchool, or eSchool).

Data Breaches

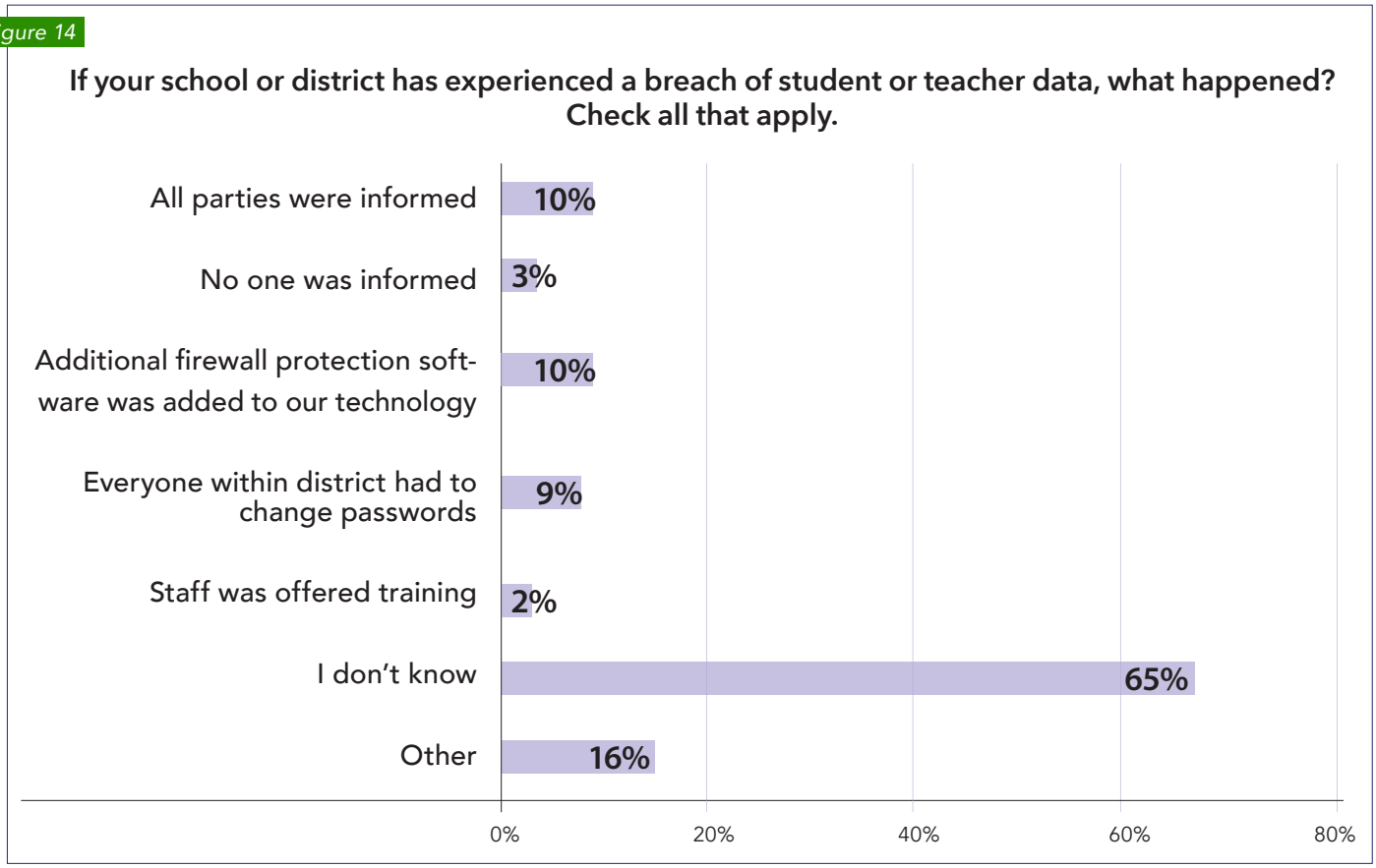
Sixty-one percent claimed they did not know if their district/school was the target of a phishing, ransomware, or cyberattack that resulted in a breach of student or teacher personal data, while 24 percent said that it hadn't been, 13 percent said teacher data had been breached, and eight percent said student data had been breached. *(Figure 13)*

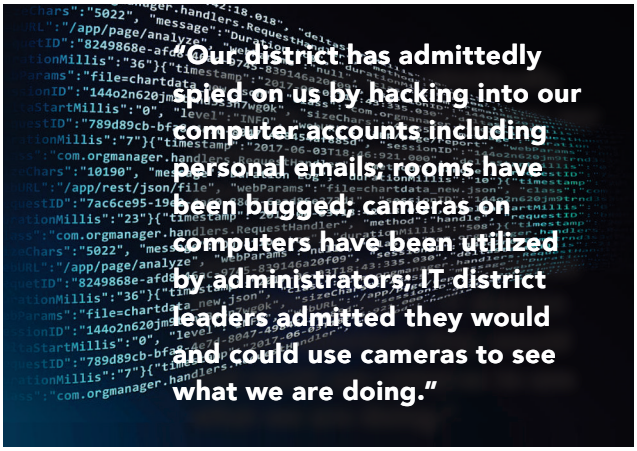
Figure 13



When asked what happens when the data was breached, 65 percent said they did not know, 10 percent said additional firewall protections were added, nine percent said employees were told to change their passwords, three percent said no one was informed, and only two percent said staff was offered training. *(Figure 14)*

Figure 14





While 49 percent reported that the district did not monitor or impinge on their privacy in a way that is concerning, 12 percent said the district does impinge on their privacy, and 10 percent reported that their district monitors their social media use even when they are not using the school computer system. One responded: "Our district has admittedly spied on us by hacking into our computer accounts including personal emails; rooms have been bugged; cameras on computers have been utilized by administrators; IT district leaders admitted they would and could use cameras to see what we are doing."

Compensation for using apps

Seventy-eight percent of educators said they did not know if their district or school regulated or restricted the practice of teachers receiving compensation from a vendor, 10 percent said there were no restrictions, and eight percent said yes, there were regulations or restrictions.

When asked if they had ever been offered money or any kind of compensation by a vendor, including travel expenses, to use, assign, promote, or evaluate an ed tech program or device, 93 percent said no. Of those educators who had been offered compensation, only one person responded that she had accepted the offer.

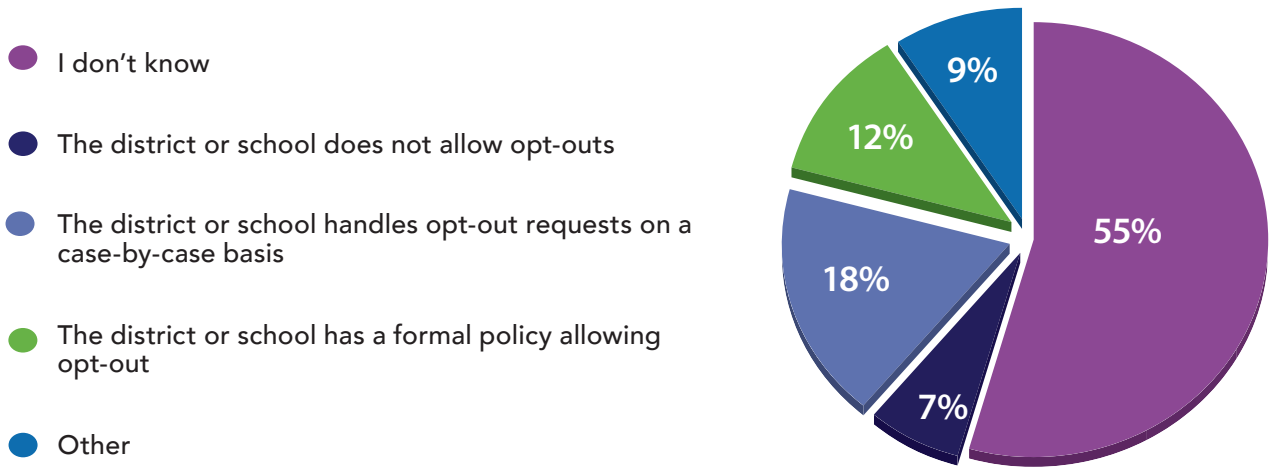
Parental knowledge and opt-out ability

Among our survey respondents, 68 percent felt that parents had little to no knowledge about student privacy, 16 percent felt they were somewhat knowledgeable, and 13 percent did not know.

Most teachers (55 percent) said they had no idea how parental opt-out requests are handled if the district required the use of apps; 18 percent said the district or school handled these requests on a case-by-case basis; and seven percent said that no opt-outs were allowed. Only 12 percent said that the district or school has a formal policy allowing opt-outs. *(Figure 15)*

Figure 15

If your district or school REQUIRES the use of education-related apps or programs, how are parental opt-out requests handled?

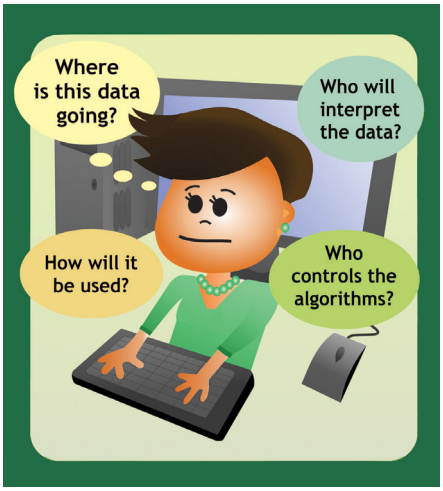


Open-ended responses

We also asked the following question: "If you think the student privacy information you received was insufficient, what was missing?" Here are some of the most common responses:

- Educators did not know which student data are being collected and how it was shared, especially when using Google Apps, Chromebooks, and PBIS (Positive Behavioral Interventions and Support Systems).
- There is insufficient training on FERPA; state, and local laws; and district policies and policies regarding student data collection and sharing.
- Teachers lack sufficient understanding on how parents can opt-out of data sharing — for example, how to opt out of sending student data to the military.
- There is outdated or inadequate professional development on how to protect privacy, with more focus on social media training than how to protect student information from being data-mined.
- Some teachers also expressed fear of being spied on by their schools or districts.

II. Focus groups



We also held several online focus groups, with a total of ten teachers and six administrators from California, Florida, New York, New Jersey, Washington, and Tennessee.

In general, their responses confirmed the findings of our survey: that educators are using more and more digital tools that collect student data, and yet they are increasingly uncertain about what happens to the data and how to protect it from breach and/or abuse. Our focus groups also allowed us to go into more depth on certain topics, such as the potential misuse of data dashboards and data walls, as well as personal experience of breaches.

The use of data dashboards, data walls, and algorithms

One of the issues that our teacher focus groups discussed was the widespread and nearly universal use of data dashboards. Many participants expressed concerns about how teachers could access prior discipline histories of students and other personal data from the dashboards that might lead to their forming negative preconceptions that could affect their relationships and expectations of their students.

Other issues related to the fear of potential breaches of sensitive health information found on the dashboards, especially in the case of students with special needs. Two teachers were worried about how this data might be utilized for marketing or commercial purposes. Finally, one told us that she was aware of some teachers who provide substitute staff and even students with their passwords and usernames to take attendance, which gives them access to private student information.

Eight out of the ten teachers interviewed had witnessed the use of data walls at their schools, in which student test scores or grades on assignments are publicly displayed in the classroom or hallway. When asked how students were identified, participants reported that identification numbers were used, and one said that in her school children's names and pictures were used. None of the participants felt that the use of data walls was positive because, they said, they shame and humiliate children and violate their privacy.

Participants were asked if they were aware that data algorithms were being used to steer student learning. Six reported yes; examples mentioned included adaptive learning programs like Dreambox.

Teacher data, breaches, and disclosures

When asked if they knew what personal information of their own the district shares with the state, five participants said no, and five had some idea of what could be shared (certification numbers, for example, and their name linked to the names and test scores of their students).

When asked if their district had ever experienced a breach, two participants said yes and eight said no. The two who had experienced a breach were asked how the issue was resolved.

One reported that the district bought LifeLock for two years, but that the staff person who had caused the breach kept her job. In the other case, teachers were not informed about the extent of the breach, just told that the system had been compromised. This participant reported that the risk of breaches had increased over the past couple of years and that the district was told that teachers need to get more training.

Another participant reported that charter schools had accessed student names and addresses from the district and that parents were only warned about this after the information had been released.

Largest concerns about data privacy

In our focus groups, the following were the largest concerns expressed about data privacy and the use of ed tech in schools:

- Teachers being forced to use a particular vendor, like Google
- Lack of transparency about how data is shared and used
- The risk that faulty data will be used to make decisions
- That students were no longer treated as individuals but as data points
- Teachers' lack of knowledge of data privacy, including where the data was going
- School leaders blindly trusting corporations

Participants also reported the following questions and concerns:

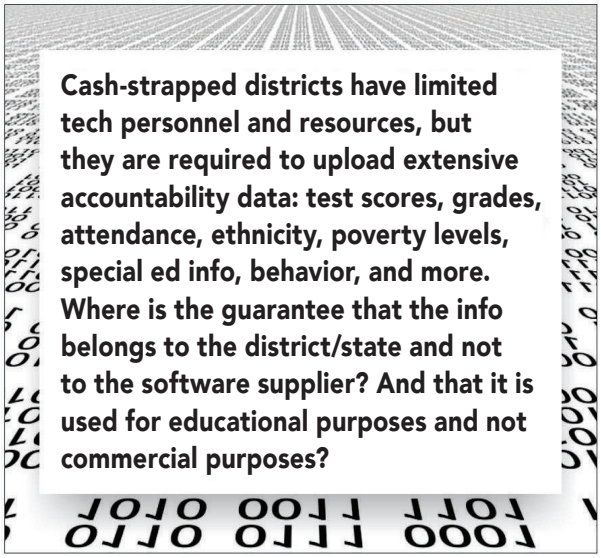
- I am concerned that districts are beginning to ask for reasons when teachers take sick days
- Data mining by vendors
- Districts monitoring social media
- District leaders not trained
- What is the union doing?
- What is the individual liability of teachers if a breach occurs?
- What are the intellectual property rights of a teacher when his/her work is shared with a vendor?
- The need for whistleblower protections for teachers who report problems with data privacy
- The need for more parent and teacher education on the issue of data privacy

III. Administrator one-on-one interviews

We also held a series of in-depth, one-on-one interviews by phone with school administrators, including three principals and three superintendents based in California, New York, and New Jersey. Each interview lasted approximately one hour.

Decision-making and use of ed tech products

We asked how they would evaluate their district in terms of a high technology, moderate technology, or low technology district. (High technology was defined as 1:1 or Bring Your Own Device programs and digital textbooks. Moderate-tech was defined as laptops are available, some online course or support material is required, and use of classroom apps is encouraged. Low-tech was defined as computer use is limited to labs or the library and required/voluntary use of online courses/apps is minimal.) Four participants rated their districts as low to moderate and two rated their districts as high-tech.



We asked participants if the use of technology was mandatory in their schools. Two said no and four said yes.

Four participants reported the district provided devices for each student.

All six reported that their district required use of specific online programs. When asked who makes decisions to use these programs, three participants reported this was the result of collaboration between the Superintendent of Curriculum, principal, instructional coach, and teachers, while three reported that teachers alone decide.

When asked if apps are evaluated prior to their use, five out of the six reported that they were not aware of any formal policy to evaluate apps.

Four participants reported that they did not know what happens when an app was discontinued, and if the student data was deleted.

One surmised it was the responsibility of the tech department to deal with this issue, and the others said there was no procedure in place.

When asked if they ever had a parent request to opt out of use of online programs or apps, three reported yes and three reported no.

Lack of sufficient knowledge of data privacy issues and laws

All but one of the administrators reported that they had not received any formal training on how to protect student data.

When asked if they were familiar with the federal laws FERPA and PPRA, all six reported they were familiar with FERPA, but three were not familiar with PPRA. When asked about their state privacy laws, three reported they knew about them and three reported they did not.

When asked if their district had restrictions on data use apart from federal or state laws or regulations, four said no, and two said yes.

Other concerns with the growing use of ed tech and data privacy

These administrators also responded that their biggest concerns about data privacy were the following:

- There is too much data! Who is watching it? I don't know and that concerns me.
- I have no confidence in the state and what they are doing with the data. I will not share data with them. If they want educational data, they can contact the parent for permission. It is not my purview to share personal data with the state.
- I am concerned because there are programs that teachers can upload to devices the school gives them that TRACK THE TEACHER!
- Teachers should not be technicians.
- We need to find the balance between technology and teaching.
- We have not done a good job of teaching our children digital citizenship.
- Data is too often monetized. Data must remain in the hands of the individual.
- Teachers need training on how to use tech and need time to develop a comfort level with it.
- Technology is moving too fast and districts are struggling to keep up.

When asked to share anything else about privacy/technology they feel we had missed in our discussions, they added the following:

- How can we better handle parent communications?
- How can we assist teachers to lockdown their online material, so students cannot access it?
- We need Teacher Digital Citizenship, so they set good examples for students.
- Teachers must make sure that they log off, so they do not fall victim to hacking.

Finally, these administrators were asked if they had any other concerns about the increased use of education technology in schools and classrooms, apart from its impact on data privacy. They reported the following:

- How the use of technology is leading to increased rates of depression, inability to communicate, and phone addiction among students.
- Free apps that ask for too much information.
- Our IT Department has access to everyone's passwords.
- Problems with student use of cellphones in school, including recording teachers in class.
- How social media posting stays with you forever and never goes away.

IV. Online products used by respondents

ABC Go
ABC Mouse
Accelerated Reader
Achieve 3000
Actively Learn
Altis Reach
Artsonia
Baseline Edge
Canvas
Castle Learning
Cayden Betzig
ClassDojo
Clicker
Code.org
CommonLit
Cool Math
Destiny
Digital Readworks
Do2Learn
Dreambox
ESchool
Edmodo
EdPerformance
Edublog
Education.com
Educreations
Edulastic
Engrade
Epic
Flipgrid
Google Apps (Documents, Sheets, Sites, Slides)
Grading Portals
Grammarly
Groupme
iReady
iStation
IXL.com
Khan Academy
Kahoot
Kidblog
Mastery Connect
Math Playground
MobyMax
MyOn
Naviance
Nearpod
News-2-You
Newsela
No Fear Shakespeare
NoredInk.com
Notability
Office 365 apps
Online Envision
Outlook
Padlet
PBS Kids
PhET
Plickers
PLTW curriculum
PowerSchool
Prezi
Prodigy
Quia
Quill.org
Quizizz

Quizlet
Raz-Kids
Read Theory
ReadWorks
Reading A-Z
Readtheory.org
Readworks.org
Reflex Math
Remind
Restaurant and coupon apps
Scholastic News
SchoolTool
Schoology
Scratch Jr.
Skyward
Socrative
Soundation
Sphero Edu
ST Math
Star Math and Reading
Starfall
Stop Motion Animator
Study Island
Sumdog
Swis.org
Synergy
Tenmarks
TimeKeeper app
Turnitin
Vernier Graphical Analysis
Weebly
WeVideo
Work sampling
XtraMath
YouTube
Zearn

RESOURCES

Badass Teachers Association's data privacy memes

http://www.badassteacher.org/bats-and-parent-coalition-for-student-privacy-teacher-privacy-toolkit-memes-to-share/

Breaches and cybersecurity incidents

https://k12cybersecure.com/

Campaign for a Commercial-Free Childhood's Children's Screen Time Action Network

https://screentimenetwork.org/

Consortium for School Networking (CoSN)

https://cosn.org/

"Data Breach Referral Memo" and "Collectively Bargained Privacy Protections in Right to Work States Memo" issued by the American Federation of Teachers (AFT) in July 2018

https://www.studentprivacymatters.org/wp-content/uploads/2018/07/Data-Breach-Referral-Memo.pdf

https://www.studentprivacymatters.org/wp-content/uploads/2018/07/Memo-Collectively-Bargained-Privacy-Protections-in-Right-to-Work-States.pdf

Data walls

https://www.studentprivacymatters.org/data-walls-must-come-down-we-will-help-parents-do-so/

https://www.washingtonpost.com/news/answer-sheet/wp/2014/02/14/how-data-walls-in-classrooms-can-humiliate-young-kids/?utm_term=.a22b209d33c8

https://www.edsurge.com/news/2018-09-07-tear-down-that-wall-why-data-walls-may-cause-more-harm-than-good

Electronic Privacy Information Center (EPIC)

https://epic.org/state-policy/student-privacy/

Electronic Frontier Foundation (EFF) advice to maximize privacy settings when using Google Chromebooks or G Suite for Education (i.e. Gmail or Google Docs)

https://www.eff.org/deeplinks/2015/11/guide-chromebook-privacy-settings-students

https://www.eff.org/deeplinks/2015/11/guide-google-account-privacy-settings-students

EFF report: "Spying on Students: School-issued devices and student privacy"

https://www.eff.org/files/2017/04/13/student-privacy-report.pdf

Fordham Center on Law and Information Policy (CLIP)

https://www.fordham.edu/info/20686/fordham_clip

Information on how Android mobile smartphone apps commonly used in school may be misusing teacher and student information

https://www.washingtonpost.com/news/the-switch/wp/2017/07/27/we-tested-apps-for-children-half-failed-to-protect-their-data/?utm_term=.1boicf5c3795

Access the searchable database of Android mobile smartphone apps:

https://www.appcensus.mobi/

Local and state union resolutions and new business items (NBIs)

https://ra.nea.org/wp-content/uploads/2016/05/Reports_on_Implementation_of_Actions_of_the_2015_Representative_Assembly_2016.pdf (see p.12)

https://www.nea.org/assets/docs/New_Business_NEA_Handbook_2018.pdf (see pp. 373 and 374)

Massachusetts Student Privacy Alliance, including contracts and model agreements with ed tech vendors

https://secure2.cpsd.us/a4l/

National Education Association (NEA) report: "Education Technology: Friend or Foe"

http://neatoday.org/wp-content/uploads/2016/06/20422-PB-Student-Data-Privacy-Ed-Tech.pdf

Network For Public Education's report: "Online Learning: What Every Parent Should Know"

https://networkforpubliceducation.org/2018/03/10345/

Parent Toolkit for Student Privacy

https://www.studentprivacymatters.org/toolkit/

Quality of life survey reports by the Badass Teachers Association and the American Federation of Teachers

https://www.aft.org/sites/default/files/worklifesurveyresults2015.pdf

https://www.aft.org/sites/default/files/2017_eqwl_survey_web.pdf

Sample privacy resolution by the Illinois Federation of Teachers

https://www.ift-aft.org/your-union/resolutions-constitution/2016-ift-resolutions/lists/2016-resolutions/resolution-no-5-appropriate-use-of-private-and-educational-data

Security risks to schools and their data systems, including recommendations for specific security protections

https://info.publicintelligence.net/FBI-CyberCriminalsSchools.pdf

https://www.ic3.gov/media/2018/180913.aspx

https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html

U.S. Department of Education guidance letters related to the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA)

https://studentprivacy.ed.gov/topic/letters-importance

U.S. Department of Education Privacy Technical Assistance Center (PTAC) document on how the Terms of Service of free websites and apps used at school may violate the Federal Educational Rights and Privacy Act (FERPA)

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf

---

And don't forget our websites:

Parent Coalition for Student Privacy at *www.studentprivacymatters.org*

Badass Teachers Association at *www.badassteacher.org*