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.

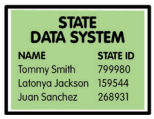
Student data is also valuable as a corporate asset. Some state laws and even the Student Privacy Pledge, a voluntary set of data principles agreed upon by 347 ed tech companies as of June 2018, specifically allow private corporations to sell student data — worth millions — in the case of mergers, acquisitions, 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

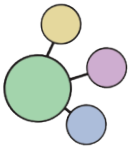
Unfortunately, it's not at all uncommon for ed tech companies to commercialize or otherwise use student data for their own purposes. At least twenty-two states, including California, Colorado, Illinois, and Virginia, have recently passed state laws specifically allowing ed tech companies that collect 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.

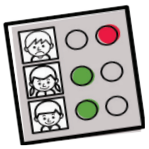
> In a 2018 report conducted by Kaplan Test Prep, 68 percent of surveyed colleges say it's "fair game" to use information gleaned from applicants' social media accounts to determine who gets accepted.



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."