# 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.

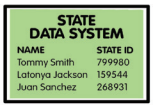
Teachers also create and share some of their own data with private companies when they use technology tools in the classroom, particularly if they're issued personal laptops or devices by the school or district. These data may include their names, email addresses, schools, photos, courses or subjects 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.

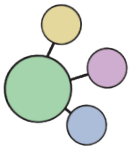

## Teacher data can be repurposed

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.