children's screen time action network

Problems with Privacy and Misuse of Student Data

The growing use of technology by schools, accelerated by the recent expansion of Cloud computing, creates serious concerns about children's privacy and the commercialization of the data collected by edtech platforms and apps. Many technology companies collect far more information on children than is necessary and store the data indefinitely. The data – collected from kindergarten to high school – may include sensitive information such as birthdates, social security numbers, disability status, behavioral information, and whether a student's family qualifies for free lunch. It can also include information gleaned from school device use, such as browsing history and contacts.

Children and their parents rarely have a say in what devices and technology programs their students use. And they rarely have the opportunity for any meaningful review of what kinds of data are collected, let alone how the data will be used. In many situations, the school employing the technology consents on behalf of the parents without their knowledge or understanding. In other cases, parents or students are directed to click on a button to consent to a complex and lengthy privacy policy written in legalese. And regardless of what's in the privacy policy, parents have no way to know whether an edtech vendor's practices actually reflect its policies.

Parents may never know the full extent of how their children's personal information may have been shared, used, misused, sold, breached, or hacked over the course of their school careers. If their children are denied entrance into the college of their choice, parents may wonder if their children's profiles were sold to universities by the College Board and ACT and used to reject their applications. If their children are turned down for their dream jobs, did the employer screen them using an online profile of their internet search history gathered by their school-issued device and purchased from data brokers? If their children's identities are stolen, was it the result of an elementary school's data breach many years ago? If their children are denied state services as an adult, could it be because of disciplinary or other incriminating information in their cumulative files held by the state education department and other agencies?

While there are federal laws – FERPA and COPPA – intended to protect children's privacy, edtech companies exploit loopholes in these laws to skirt consent, reporting, and data minimization requirements, sometimes through deceptive practices. As in many other privacy matters, the deceptive exceptions are now the true operating rule.

Parents' and advocates' concerns over the misuse and security of their children's private data center on the following issues:

Lack of Transparency: Sometimes devices are issued to students without parents' knowledge or consent. Parents are seldom informed about what apps their kids are required to use, what data is being collected, and how the data is used. With no notice or help from schools, parents are left on their own to understand the privacy implications of the technology's use. When they request this information, they are often stonewalled. And even when parents are provided with privacy policies and asked for their consent, the policies are often difficult to understand,

evasive, and incomplete. For instance, many privacy policies for edtech services do not explain why particular data are collected from students and contain unhelpful information like, "We may share this information with third parties" without ever naming those third parties or specifying why they need access to a student's personal information.

Sale of Data to Commercial Interests: There is a thriving marketplace for student data, including sensitive information such as age, gender, location, ethnicity, religion, and hobbies. These data, which are brokered and auctioned to the highest bidders, allow commercial interests to profile and stereotype our children, and manipulate them for corporate profit and, potentially, other purposes. This typically happens without parent consent.

Data Breaches: As demonstrated by several major data breaches in the last few years, the public sector is relatively unsophisticated regarding securing the data that is collected – both by themselves and by the various software packages they employ. In many situations they are hampered by funding limitations. For example, unlike many private corporations, few, if any districts hire a single full-time employee dedicated to privacy. This lack of effective security makes children's data susceptible to being stolen by people with malicious purposes, such as identity theft, discrimination, predation, or even blackmail. Likewise, edtech vendors themselves often skimp on encryption and other data security measures. In 2019, a Pearson data breach exposed the personal information of students at more than 13,000 schools; to make matters worse, Pearson waited several months to announce the breach publicly.

Lack of Choice: Even if a parent chooses to opt out of the use of a particular device or software, schools are often unwilling or slow to accommodate them. Parents are forced into adversarial relationships with the very people they count on to protect their child's best interest. Even if opting out is possible, families risk the child being isolated in the classroom without suitable replacement curriculum.

Further Reading and Resources:

Parent Toolkit for Student Privacy. By Campaign for a Commercial-Free Childhood and Parent Coalition for Student Privacy. Published online May 2017.

Educator Toolkit for Teacher and Student Privacy: A Practical Guide for Protecting Personal Data. By Parent Coalition for Student Privacy and the Badass Teachers Association. Published online October 2018.

Spying on Students: School-Issued Devices and Student Privacy. By Gennie Gebhart, Electronic Frontier Foundation, April 13, 2017.

To Take Action:

Tools for Parents

Tools for Educators