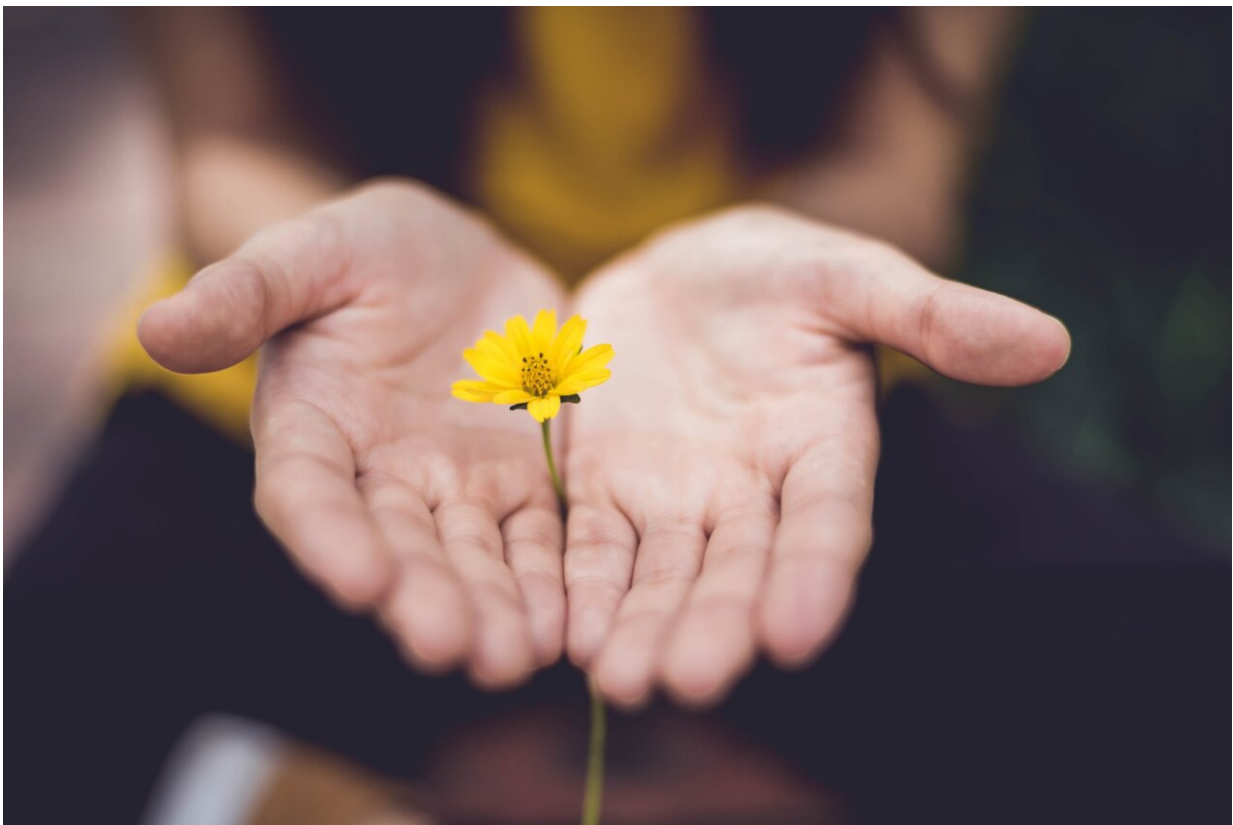


The coronavirus pandemic has forced parents' hands on data collection and privacy issues

April 9 2021, by Claudiu Popa



Credit: Unsplash/CC0 Public Domain

With the return to remote learning during the third wave of the COVID-19 pandemic, parents and students are agreeing to risky data

collection practices and privacy-invasive technologies. This unprecedented collection of data includes [video recordings of student's interactions with their teachers, collection of health information such as whether an absence is related to COVID-19 symptoms, system log-in time and student chat history](#).

The [2018 Auditor General's report on cybersecurity](#) raised many concerns about technology in schools. Many—if not most—Ontario [school boards](#) struggle to grasp the basic concepts of cybersecurity and privacy, let alone ensure that teachers are properly educated to protect [student](#) information. The report reveals that a surprising 74 percent of respondents indicated that they do not provide formal security or privacy training to staff who use technology at boards and schools.

Fifty percent of [school](#) boards inspected lacked "sufficient oversight of their classroom IT assets, such as laptops and tablets, to keep track of them. In some cases, board staff were unable to verify whether any equipment was missing."

Trading information

If keeping track of physical assets is such a challenge, even less likely is the due care and protection of the vast amounts of gathered information collected and shared with tech firms and their partners.

Student data is no longer limited to a name and a student number. It now includes precise location information, sensitive communications, classroom photos, contact information and details of health conditions. Many other facets of children's identities are collected and tracked across the student's academic life and shared with anyone who has access to the technologies adopted by [school administrators](#).

Many of these technologies are the brainchild of opportunistic

entrepreneurs, developed by interface designers with little to no understanding of privacy and security. Worse yet, they have been adopted by untrained school board administrators using procurement processes that not only predate the pandemic, but also the internet itself.

Tracking industries

Most students have already been enrolled in online classes, registered with videoconferencing tools and continue to be tracked using invasive data collection methods. Indeed, student information systems or student management systems often aggregate all identity and academic information and store it outside the traditional confines of school board servers. This cloud-based data processing allows providers to partner with unnamed parties to analyze collected data.

Sometimes, this information is even shared back with the school boards themselves, ostensibly with an eye towards improving education.

Although the early years of educational technologies (edtech) were rocky, with [vast breaches impacting millions of students worldwide, the industry managed to survive.](#)

Many of the companies that built their models on data collection are still around, [now valued at hundreds of millions of dollars.](#)

No opt-outs

This situation has proved to be a different beast, with regulations and privacy legislation tightening around rapacious edtech firms. Publicly funded boards of education that have enjoyed no regulatory oversight have now started to examine their practices.

Here, the expansion of school board authority is presented under the guise of privacy and safety. Rhetoric such as "synchronous learning tools," "digital tools" and "communication tools for student and family engagement."

Fearing that their information collection and sharing practices might expose them to liability, school board administrators are abruptly putting their foot down. But requests for [parental consent](#) do not include an option to decline, or the presentation of a viable alternative. This coercion includes disciplinary implications for students whose parents opt out.

[School boards refer to the Education Act](#), which pre-dates the internet, for the authority to share student data as they see fit and without seeking additional consent.

Parents should take a stand and protect their families by requiring school boards to supply sufficient [information](#) to be comfortable with relinquishing the digital identities of their children to a variety of strangers. Parents can also request urgent investigation into the veiled threats of discipline and marginalization made by school boards towards students.

Claudiu Popa, Author and Lecturer in Fintech Cybersecurity, Information Risk and Enterprise Privacy Management, *University of Toronto*

This article is republished from The Conversation under a Creative Commons license. Read the original article.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: The coronavirus pandemic has forced parents' hands on data collection and privacy issues (2021, April 9) retrieved 26 April 2024 from

<https://techxplore.com/news/2021-04-coronavirus-pandemic-parents-privacy-issues.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.