Stop Google's Kiddie Data Predators

No consent. No disclosure. No escape.

Published: Wednesday, 26 September 2018 07:49

By Michelle Malkin

Hits: 2766

For legions of unwitting students and teachers across the country, this is the dangerous, de facto data policy Google has imposed over their school districts. An estimated 80 million students and teachers are now signed up for free "G Suite for Education" accounts (formerly known as Google Apps for Education); more than 25 million students and teachers now use Google Chromebooks. A Google logon is the key to accessing homework, quizzes, tests, group discussions, presentations, spreadsheets and other "seamless communication." Without it, students and teachers are locked out of their own virtual classrooms.

Local administrators, dazzled by "digital learning initiatives" and shiny tech toys, have sold out vulnerable children to Silicon Valley. Educators and parents who expose and oppose this alarmingly intrusive regime are mocked and marginalized. And Beltway politicians, who are holding Senate hearings this week on Big Tech's consumer privacy breaches, remain clueless or complicit in the wholesale hijacking of school-age kids' personally identifiable information for endless data mining and future profit.

Over the past several years, I've reported in my column and CRTV.com investigative program on edutech plundering the personal data and browsing habits of millions of American schoolchildren. Remember: State and federal educational databases provide countless opportunities for private companies exploiting public schoolchildren subjected to annual assessments, which exploded after the adoption of the tech industry-supported Common Core "standards," tests and aligned texts and curricula. The Every Student Succeeds Act further enshrined government collection of personally identifiable information -- including data collected on attitudes, values, beliefs and dispositions -- and allows release of the data to third-party contractors thanks to Obama-era loopholes carved into the federal Family Education Rights and Privacy Act.

The racket includes Facebook's Digital Promise partnership with the U.S. Department of Education and the social/emotional behavior tracking system of TS Gold (Teaching Strategies Gold) targeting preschoolers. Yes, preschoolers. The Big Business-driven Project Unicorn promotes "data interoperability" between and among a cornucopia of edutech products vying for your kid's clicks and data. And despite getting caught data-mining students' emails without consent, Google continues to infiltrate classrooms and family rooms.

Parents, did you get notice before your child signed on to a Google account? In many districts, school information officers usurp your family authority and are logging on your sons and daughters en masse without your consent or knowledge. You don't get to see the terms of service, the privacy policy or the G Suite agreement between Google and your school. Even if parents do receive notice before their kids are dragooned into G World, opt-out mechanisms are nonexistent or nearly impossible to navigate.

Springfield, Missouri, public schools employee and parent Brooke Henderson, along with her sister, Brette Hay (who is also a mom and educator), were horrified to discover that even if they logged

Stop Google's Kiddie Data Predators

Published: Wednesday, 26 September 2018 07:49
By Michelle Malkin
Hits: 2766

out of their G Suite accounts, their personal passwords, bank account information, parents' personal data, spouses' sensitive data and children's browsing habits were being stored on district-issued Google Drive accounts. Unbeknownst to the sisters, Google's auto login and auto-sync functions allow the collection and archiving of non-education-related information across the extended family's devices.

Henderson showed me screenshots and videos of these breaches, including storage of her young niece's personal voice-to-text searches and memos and her nephew's YouTube viewing records. Even worse, such information is accessible to unknown numbers of district employees. The security concerns are multiplied and exacerbated by other third-party data management systems used by Henderson's district that "play well" with Google, such as Instructure's program Canvas and single sign-on program Clever.

As parent privacy advocate and researcher Cheri Kiesecker asserts: "Parents don't want to just see businesses' policies after they get our kids' data. We want to have consent whether they get the data, and students should not be penalized if parents choose not to share data. There also should be an enforceable penalty if data is misused."

Message to Congress: Allowing Google to dictate "frameworks" for education information grabs is like letting the fox guard the henhouse. Parents have a right to know -- and the right to "NO" -- when it comes to protecting their children's privacy. Anything less is capitulation to kiddie data predators.

This column is Part I of a new series on "The EduTech Data Heist." Michelle Malkin is host of "Michelle Malkin Investigates" on CRTV.com. Her email address is writemalkin@gmail.com.