



## Beware of Big Bathroom Brother

Nine years ago, I warned readers about “eyelock biometric readers” adopted by Florida schools to track them on buses. Under the guise of fighting guns and vaping, countless schools this year are now installing surveillance sensors in bathrooms that can spy and record students’ alleged “aggression” and red-flag “spoken key words.”

Eight years ago, I warned readers about a company called Teaching Strategies Gold that created an “early childhood assessment system” for “social emotional, physical, language and cognitive development” that documents student behaviors with videos, audio files, journals and photos — which are then uploaded to a central database cloud. In Jefferson County, Colorado, TS Gold was used to monitor and shape preschoolers’ bathroom trips, hand-washing habits and other “socially acceptable behavior.”

Three years ago, I warned readers about a company called e-Hallpass and the increasing student health data mining hijacking America’s schools. As I reported at the time, my then-high school sophomore son’s public high school in Colorado Springs told every student to download e-Hallpass, which is seamlessly connected to every student’s mandatory Google login, to track how much time students spend in the bathroom. It was done all in the name of “safety,” of course, with no parental consent.

Biometric surveillance edu-technology has spread rapidly, with fingerprint and facial recognition tools proliferating worldwide on K-12 and college campuses as a result of the COVID global track-and-trace regime and pandemic profiteers. In 2020, I noted the spread of “electronic beacons” to track student movements and apps like Google’s ClassDojo, which mines intimate student behavioral data and creates long-term psychological profiles that can be shared and sold to third parties unbeknownst to kids and their families. The Pioneer Institute reported that government at all levels had spent \$30 billion in 2018 on such intrusive, brainwashing “social-emotional learning” surveillance in K-12.

Over the years, my incessant warnings about the Edutech surveillance machine have been mocked, belittled, attacked and ignored as baseless “paranoia” and “conspiracy”-mongering by the likes of the anti-right, anti-white, anti-parent Southern Poverty Law Center.

But now, the truth is permeating the mainstream. As the school year ramps up, watchdogs have finally discovered insidious little behavior modification tools like e-Hallpass masquerading as protection measures.

The Arizona Informer tweeted this week that Pinnacle High School in Paradise Valley, Arizona, will use e-Hallpass to track social distancing and other student movements with no parental consent.



Gage Skidmore/Wikimedia Commons  
Michelle Malkin



Written by [Michelle Malkin](#) on August 17, 2022

---

A Twitter user named @hannahposts wrote this week: “Looks like school is gonna make us use eHallpass, the program where we track how long, at what time, and how often each child goes to the restroom and store that information on third party servers run by a private for-profit company.... If you’re a parent and your kid’s school uses e-hallpass, politely yet firmly ask for your kid to be opted out. If we have enough opt outs the system won’t work.”

Security researcher Peter Lowe, who is now belatedly awake to e-Hallpass, also tweeted important fundamental questions this week that every parent should be asking:

“Hey @Software4Ed, the privacy policy which you use for e-hallpass states that you release data to third parties ‘working directly with Eduspire Solutions to support our software’. Which third parties are those? Can you provide a full list?”

And one online student petition calling for repeal of the e-Hallpass system at Lewisburg Area High School in Lewisburg, Pennsylvania, blew the whistle on how “E-hallpass knows your age, who your parents are, who your friends are, what classes you’re taking, and what classes you’re struggling in. That’s a lot of very sensitive information the school is forcing you to give to this company, leaving it vulnerable for hackers to hold for ransom, or to sell to identity thieves so they can ruin your life.”

Beware of Big Bathroom Brother. He’s not in Beijing or Moscow or Pyongyang. He’s here, clothed in public service and public safety, sacrificing your children’s autonomy and serving the Silicon Valley masters of American “capitalism.”

*Michelle Malkin’s email address is [MichelleMalkinInvestigates@protonmail.com](mailto:MichelleMalkinInvestigates@protonmail.com). To find out more about Michelle Malkin and read features by other Creators Syndicate writers and cartoonists, visit the Creators Syndicate website at [www.creators.com](http://www.creators.com).*

COPYRIGHT 2022 CREATORS.COM



## Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



[Subscribe](#)

### What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.