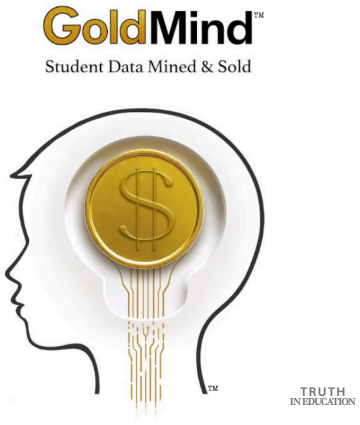


SILENT SURVEILLANCE – Who is Watching Your Child?

AI student surveillance software has broad collection capabilities, and student data collected by AI student surveillance software is not kept private. These capabilities combined with the lack of data privacy can harm the very children the companies claim to protect.

The Broad Capabilities of Student Surveillance Software

While it is no surprise that parents and schools are concerned with student violence, bullying, and self-harm, most would be shocked to realize that the Education Technology (EdTech) industry intentionally propagates these fears to sell their products as the answer to student safety.[1] This has led to a boom in the EdTech student surveillance industry, currently valued at $8 trillion.[2] This is further bolstered by over $300 million in federal funding secured through lobbying efforts and political pull.[3] This federal funding is often used to bring the surveillance software to schools, as it helps to mitigate the startup costs associated with purchasing and implementing the technology.

The emergence of student surveillance programs such as Gaggle, Lightspeed, Bark, Securly, and GoGuardian have begun to cause concern for parents and civil rights experts alike. These programs are installed on student devices and school logins, running in the background to covertly scan everything a student does, using a search algorithm programmed to alert designated authorities when certain keywords or phrases are used by students. Common features of surveillance software include AI-driven behavioral detection, social media monitoring, student communications monitoring, online and web monitoring, and remote video monitoring/proctoring.[4]

---

[1] *Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling*, AMERICAN CIVIL LIBERTIES UNION 4 (2023), https://assets.aclu.org/live/uploads/publications/digital_dystopia_report_aclu.pdf.
[2] *The World's Largest EdTech Community*, ASU+GSV (2026), https://www.asugsvsummit.com/.
[3] *Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling*, AMERICAN CIVIL LIBERTIES UNION 5 (2023), https://assets.aclu.org/live/uploads/publications/digital_dystopia_report_aclu.pdf.
[4] *Id.* at 9, 10.

AI-driven behavioral detection uses video to analyze a student's visual behavior, triggering warning flags to school officials when "problematic" behavior is observed. Social media and student communications monitoring look for "red flag" terms or phrases as they scan student social media posts, chats, documents, comments, emails, and more – even off campus after school hours, so long as the student is using their school-issued device or account with the software. Online and web monitoring includes flagging and blocking websites deemed to be problematic or unsafe, triggering reports with school authorities when they are accessed. Remote video monitoring/proctoring software allows a device to use its camera to monitor the student for attendance, focus, and cheating.[5] These examples of student surveillance software only apply to the security realm of EdTech products and can be combined with mental health products such as MindLift, which uses facial expression analysis, sentiment analysis, and behavioral monitoring to predict a student's mood or mental health state.[6]

One popular student surveillance software is Gaggle, which integrates into widespread education apps such as those provided by Google and Microsoft. This software provides an example of the confusing (and potentially deceptive) language used by EdTech surveillance companies when describing its capabilities and data collection. Though Gaggle states that it "does not monitor students' social media accounts, personal email accounts, personal devices, or web browsers," its website continues to state that "It only monitors content and activity, such as documents or chat messages, produced using a school-owned device, email address, or online tools within Google Workspace for Education, Microsoft 365, Google Chat, Microsoft Teams, and the Canvas learning management system."[7] This statement implies that the first items are not monitored at all but negates to inform the user of the many exceptions to these claims. Thus, the same conduct on a school-issued device or account (even using a personal device) is most certainly monitored by the software:

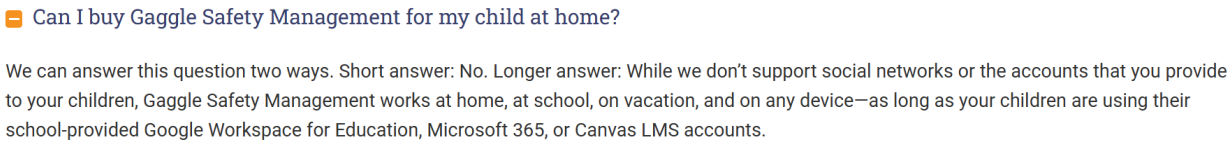
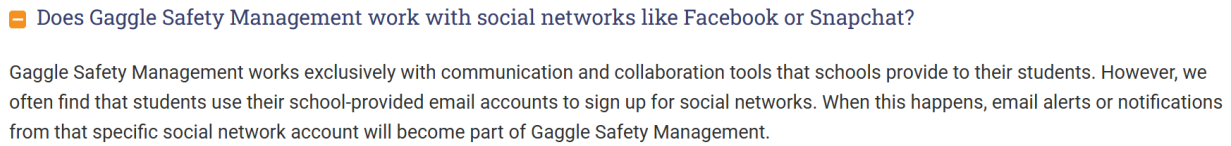


Image from Gaggle's Frequently Asked Questions for Parents[8]



---

[5] *Id.*
[6] Shanky Goyal et al., *MindLift: AI-Powered Mental Health Assessment for Students,* 5 NEUROSCIENCE INFOMATICS 1, 1 (Jun. 2025), https://www.sciencedirect.com/science/article/pii/S2772528625000238.
[7] *Student Trust and Privacy Center,* GAGGLE (2025), https://www.gaggle.net/trust-and-privacy-center.
[8] *Frequently Asked Questions,* GAGGLE (2025), https://www.gaggle.net/frequently-asked-questions.

Image from Gaggle's Frequently Asked Questions for Educators[9]

Contradictory language can be found throughout the Gaggle Student Data Privacy Notice, often in the form of affirmative statements immediately followed by exceptions[10]:

- After describing FERPA protections limiting student data shared with third-party entities, Gaggle then informs the user that it qualifies as an exception, as it is "acting as a school official with legitimate educational interest . . . and is using student data only for an authorized purpose and in furtherance of such legitimate educational interest."
- **"**Data is never shared with unrelated third parties for research, although de-identified data is used to improve the product"
- "User identity is not linked to other sources, except student information systems as provided by the school or district"
- "Gaggle does not combine personally identifiable information except for data produced by the school or district."
- "Users do not create or upload data on Gaggle but may do so via the platforms being monitored."

Other data collected by Gaggle include student and parent/guardian first and last names, physical address and email address, along with parent/guardian phone numbers, student ID, and the "approximate location of a student [as] collected through the Gaggle browser extension." *Id.*

Is Student Surveillance Data Private?

Coupled with the broad surveillance capabilities of student surveillance software is the data that is collected and stored for each student. While companies claim it is anonymized, the sheer amount collected creates a behavior profile that can be easily linked to an individual student, much like how ad data is able to be linked to individual internet users.

Parents have reportedly felt uninformed about the data collected on their students and the extent to which surveillance is conducted, feeling that notification and consent was either nonexistent or "buried [in] long technology use forms" of which opting out was either not authorized or unfeasible. [11] Parents lose even more control over their child's data due to the fact that federal regulations do not explicitly limit the data companies can collect on students, and FERPA exemptions are granted to the surveillance companies.[12] [13] Gaggle drives this point home in its privacy notice, stating that "Parental consent with respect to third parties does not apply as .

---

[9] *Id.*
[10] *Student and Staff Data Privacy Notice,* GAGGLE (2025), https://www.gaggle.net/student-data-privacy-notice.
[11] Sharon Lurye & Claire Bryan, *Takeaways from Our Investigation on AI-Powered School Surveillance,* AP NEWS (Mar. 12, 2025), https://apnews.com/article/ai-school-chromebook-surveillance-gaggle-investigation-takeaways-381fa82978f27eb85f20d03236820711.
[12] Jessica Paige et al., *Schools Let AI Spy on Kids Who May Be Considering Suicide. But at What Cost?,* TIME (Feb. 15, 2024), https://time.com/6694425/ai-monitoring-school-suicide-cost-essay/?utm_source=chatgpt.com.
[13] *Student and Staff Data Privacy Notice,* GAGGLE (2025), https://www.gaggle.net/student-data-privacy-notice.

. . consent is provided by the school or district," which "operating *in loco parentis* control all student information and privacy settings." [14]

Companies such as Gaggle design their privacy notices to explicitly warn of the possibility of breaches, including statements that "neither we nor any other hosted service provider can guarantee the security of all personally identifiable information."[15] And mistakes certainly do happen, as the Associated Press reported in 2025 when Gaggle accidentally released 3,500 unredacted documents containing sensitive student data in response to an Open Records Request submitted by the publication. [16]

Gaggle is by no means alone in its breaches, as even Google's G Suite education platform recently settled a class action lawsuit for $8.75 million following allegations that it unlawfully collected and stored student biometric data without parental knowledge or consent. [17] Even the United States Office of Personnel Management Office was compromised by Chinese hackers in 2015, releasing over 22 million files containing the highest level of security clearance information for military, federal, and contractor personnel. These documents included detailed information of the applicants and their contacts, including background investigation records documenting personal disclosures such as drug use and sexual activity. [18] The SolarWinds breach in 2019 followed suit, compromising the data of thousands of organizations along with the departments of Homeland Security, State, Commerce and Treasury.[19]

While EdTech surveillance companies will always market their intentions to keep student data safe, intentions and safeguards cannot always prevent breaches. Parents who truly wish to protect their child's personal data may find that the only way to do so is to ensure that it is never collected in the first place.

How AI Student Surveillance Harms the Children it Claims to Protect

Aside from the risks of compromising student data and building student data profiles, many stakeholders in the education realm have shared additional concerns about student surveillance software.

---

[14] *Id.*
[15] *Student and Staff Data Privacy Notice,* GAGGLE (2025), https://www.gaggle.net/student-data-privacy-notice.
[16] Sharon Lurye & Claire Bryan, *Takeaways from Our Investigation on AI-Powered School Surveillance,* AP NEWS (Mar. 12, 2025), https://apnews.com/article/ai-school-chromebook-surveillance-gaggle-investigation-takeaways-381fa82978f27eb85f20d03236820711.
[17] Kelsey McCroskey, *$8.75M Google Settlement Resolves Class Action Lawsuit Over Alleged Chromebook Privacy Violations*, CLASSACTION.ORG (Aug. 1, 2025), https://www.classaction.org/news/8.75m-google-settlement-resolves-class-action-lawsuit-over-alleged-chromebook-privacy-violations.
[18] Sean Bigley, *A Decade After the OPM Hack, Questions Remain*, CLEARANCE JOBS (Aug. 11, 2024), https://news.clearancejobs.com/2024/08/11/a-decade-after-the-opm-hack-questions-remain/.
[19] Saheed Oladimeji & Sean Kerner, *SolarWinds Hack Explained: Everything You Need to Know*, TECH TARGET (Nov. 3, 2023), https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Teachers worry that surveillance undermines their connection with their students, creating an air of distrust between students and the authority figures in their schools.[20] [21] This lack of trust leads teachers to be concerned that students will "shut down" rather than share their troubles, resulting in them being less likely to connect with the help and services they need.[22] Parents are concerned as the surveillance software can directly flag law enforcement, resulting in emotionally distressing situations where police officers appear for the child at home or school – especially if the trigger is deemed to be a false flag.[23] Students themselves express signs of self-censoring as they adjust their actions and behaviors to ensure that it does not trigger a "red flag" situation.[24]

Perhaps the highest price paid for EdTech surveillance software is that a generation of students is consequently being raised in a surveillance culture. They are being trained to believe that their society and peers are inherently dangerous, and for some it becomes a self-fulfilling prophecy. Students, aware of being watched, make decisions based upon the avoidance of negative consequences rather than growing in understanding of a true moral framework.[25] Constant surveillance becomes normalized, along with the perpetual anxiety which accompanies it, and students are left to conclude that privacy must be traded for safety as a fact of life.[26] This opens the door to increased, unchallenged societal surveillance at large – a future which should reek of dystopia to all citizens.

Companies – and thus their school district customers – will always argue that the surveillance is necessary, citing success stories that "tug at administrators' heart strings, presenting one-off success stories as the rule, instead of the exception."[27] However, numerous studies, to include a US Department of Justice review of the data, prove that these claims are grossly overstated with no evidence that the presence of surveillance technology contributes to safer schools. [28]

As succinctly stated in one report: "School districts should not view EdTech Surveillance companies as their allies, partners, or saviors in pursuing that [safety] goal. Each is simply a company trying to sell you a product. No more and no less."[29]

---

[20] Abdulrahman M. Al-Zahrani, *Unveiling the Shadows: Beyond the Hype of AI in Education*, 10 HELIYON 1, 3 (May 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11087970/pdf/main.pdf.
[21] *Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling*, AMERICAN CIVIL LIBERTIES UNION 23 (2023), https://assets.aclu.org/live/uploads/publications/digital_dystopia_report_aclu.pdf.
[22] *Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling*, AMERICAN CIVIL LIBERTIES UNION 23 (2023), https://assets.aclu.org/live/uploads/publications/digital_dystopia_report_aclu.pdf.
[23] Sharon Lurye, *Students Have Been Called to the Office — And Even Arrested — for AI Surveillance False Alarms*, AP NEWS (Aug. 8, 2025), https://apnews.com/article/ai-school-surveillance-gaggle-goguardian-bark-8c531cde8f9aee0b1ef06cfce109724a
[24] *Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling*, AMERICAN CIVIL LIBERTIES UNION 21 (2023), https://assets.aclu.org/live/uploads/publications/digital_dystopia_report_aclu.pdf.
[25] *Id*. at 21.
[26] *Id*. at 20.
[27] *Id*. at 17.
[28] *Id.* at 5.
[29] *Id.* at 19.

What Parents Must Do

Parents must first understand the broad reach of AI student surveillance software and have a full understanding that their student's collected data is not kept private. They can begin by questioning their child's school about what student surveillance software is used, what data can be collected, what data has already been collected, and what data the school has shared with the companies. They can request the company and/or application's privacy policies, a copy of the contract documents signed with the school district, and all other pertinent documents outlining who is responsible for the safeguarding of data and how this will be done. Additionally, parents can request that their child be opted out of the programs.

Parents may find, however, that school districts may make this difficult to do or even outright decline to produce documents, citing proprietary agreements with the company and similar contestations. School districts may also decline an opt out, citing it as an unreasonable accommodation. In these cases, Truth In Education invites parents to reach out for individualized assistance, and we will be happy to provide additional help.

Most importantly, parents must recognize the potential harms which could affect their child as a result of student surveillance software. Not only is a student's childhood documented into a school data profile and shared with unknown parties, students living in a surveillance culture live in a heightened, perpetual state of anxiety which they begin to believe is normal. If safety of students is truly the priority, then parents must keep that in mind as they make decisions of where their child is to be educated.

Truth In Education
info@truthineducation.org
404-384-2583