NO PREP

Should Schools Use AI to Watch Students?

Includes: Student reading, case study, differentiated questions, teacher key

Name: Period: Date:

Should Schools Use AI to Watch Students?

A New Kind of Classroom

In schools across the United States, artificial intelligence is watching. AI-powered surveillance cameras scan hallways and identify students who enter without authorization. Keystroke logging software monitors what students type on school-issued devices, flagging content that algorithms identify as threatening, self-harming, or academically dishonest. Facial recognition systems track attendance. Emotion recognition tools —

Name: **Period:** **Date:**

Should Schools Use AI to Watch Students?

A New Kind of Classroom

In schools across the United States, artificial intelligence is watching. AI-powered surveillance cameras scan hallways and identify students who enter without authorization. Keystroke logging software monitors what students type on school-issued devices, flagging content that algorithms identify as threatening, self-harming, or academically dishonest. Facial recognition systems track attendance. Emotion recognition tools, used in some international schools, claim to detect whether students are engaged or distressed by analyzing their facial expressions. Social media monitoring programs scan students' personal accounts for content that the school considers concerning. These tools accelerated significantly during and after the COVID-19 pandemic. When schools shifted to remote learning in 2020, proctoring software became widespread: tools that monitor students taking tests from home by activating their cameras, tracking their eye movements, and flagging unusual behavior as potential cheating. Many districts retained or expanded these tools after returning to in-person instruction. Proponents argue that these surveillance systems protect students from threats, maintain academic integrity, and help identify students in crisis. Critics argue that they create a fundamentally different educational environment, one that normalizes constant monitoring and disproportionately harms students from already-marginalized communities.

Proctoring Software and the Equity Problem

Online proctoring software like Proctorio, ExamSoft, and Respondus Monitor became ubiquitous during remote learning and remain in use at many institutions. These tools use AI to analyze students' facial expressions, eye movements, background environments, and typing patterns to flag suspicious behavior for human review or automated score nullification. Students who are flagged may face academic

consequences or be required to retake exams. The equity concerns with these tools are substantial and documented. The facial recognition components of some proctoring software perform less accurately on darker-skinned faces, meaning Black and Latino students are more likely to be falsely flagged. Students who take exams in shared family spaces, with siblings present, or without a private quiet room are flagged for environmental conditions over which they have no control. Students with anxiety disorders, autism, or ADHD have reported that the experience of being watched and analyzed causes significant distress that affects their performance. In 2020 and 2021, students at multiple universities filed formal complaints arguing that proctoring software discriminated against them on the basis of race and disability.

Keystroke Logging and the Right to Think Privately

Bark, Gaggle, and similar products are used by thousands of school districts to monitor what students write on school-issued devices. These tools use natural language processing to flag messages, documents, and searches that suggest bullying, self-harm, threats, or cyberbullying. When a flag is triggered, a human reviewer at the company examines the content and may alert school administrators or, in cases involving safety threats, law enforcement. Supporters point to cases in which these tools identified students at serious risk of self-harm or violence in time to intervene. The companies report thousands of cases annually in which their alerts led to wellness checks that may have prevented harm. Critics raise several concerns. First, the monitoring extends to content that students write and delete, including private journal entries and unsent messages, without students or parents always being clearly informed. Second, the tools generate many false positives: students writing fiction, studying violent historical events, or simply venting to a friend are regularly flagged and referred for review. Third, the knowledge that their words are monitored may cause students to self-censor: to avoid writing about mental health struggles, asking questions about sexuality or identity, or researching sensitive topics they need to understand.

Facial Recognition in Schools

At least a dozen school districts in the United States have deployed facial recognition technology for purposes including identifying unauthorized individuals entering campuses, tracking student attendance, and — in a few highly controversial cases — monitoring for students who have been suspended or otherwise flagged. In

2020, the Lockport, New York school district became the center of a national controversy when it deployed a facial recognition system using a database that included registered sex offenders and suspended students. The New York Civil Liberties Union challenged the system, and the state eventually required schools using facial recognition to undergo a formal approval process. The accuracy concerns that affect facial recognition in law enforcement apply equally in schools — systems perform less accurately on darker-skinned faces. A student wrongly identified as a threat or as an unauthorized intruder could face humiliating or traumatic consequences. In an environment where students are already navigating complex social dynamics, false alerts by surveillance systems can cause significant harm. Some civil liberties advocates argue that the most significant harm from facial recognition in schools is not individual false positives but the normalization of constant biometric surveillance during childhood — training students to accept monitoring as an ordinary feature of institutional life.

The Consent and Data Problem

Most school surveillance systems collect data about students who are minors. FERPA — the Family Educational Rights and Privacy Act — protects student educational records but does not clearly cover all data collected by third-party educational technology vendors. Many school contracts with surveillance technology companies allow those companies to retain and use student data for purposes beyond the school's oversight. Students typically have no choice about whether to participate in school surveillance systems — their devices, their campuses, and in some cases their social media accounts are monitored as a condition of enrollment. The research on whether school surveillance systems actually improve safety is limited and contested. A 2019 report by the Brennan Center for Justice found that many school surveillance programs were implemented without evidence of effectiveness and without adequate assessment of potential harms. Researchers studying school climate have found that high levels of surveillance can reduce students' sense of trust in their school and belonging within it — factors that are themselves associated with dropout rates and poor academic outcomes. The tools deployed to protect students may, in some cases, be undermining the conditions under which students thrive. Underlying many debates about school surveillance is a deeper question about what schools are for. If schools are primarily risk-management

institutions — environments whose primary goal is to prevent the worst possible outcomes — then surveillance tools that reduce the probability of extreme events may seem worthwhile even at significant cost to the educational environment. But if schools are developmental institutions — environments designed to help young people grow, take intellectual risks, develop identity, and learn to trust institutions — then the calculation changes. A school that systematically monitors students' communications and expressions may prevent some harms while undermining the conditions of trust, exploration, and authenticity that make education meaningful. Students cannot become critical thinkers, honest self-reflectors, or engaged citizens in an environment that has taught them to self-censor everything they write.

Key Information: AI Surveillance in Schools

Detail	Information
Common school AI tools	Surveillance cameras, keystroke loggers, proctoring software, facial recognition, social media monitors
COVID-19 acceleration	Remote learning in 2020 drove rapid expansion of AI proctoring and monitoring tools
Proctoring equity concern	Tools flag students with no private space; less accurate on darker-skinned faces
Bark and Gaggle	Keystroke monitoring products that flag potential self-harm, threats, and cyberbullying
Self-censorship risk	Students may avoid writing about mental health, identity, or sensitive topics if monitored
Lockport, NY case (2020)	School district deployed facial recognition; challenged by NYCLU; state required approval process
FERPA limitation	Protects educational records but not all data collected by third-party EdTech vendors
Brennan Center 2019 report	Found many school surveillance programs lacked evidence of effectiveness or harm assessment

Case Study: Miguel's Flagged Essay

Miguel is 15 years old and was assigned to write a personal narrative in English class about a moment that changed him. He wrote about a period two years ago when he was depressed and had thoughts of self-harm. He did not act on those thoughts, found support from a family member, and recovered. He wanted to write about the experience honestly because he had worked through it and was proud of how far he had come. He wrote the essay on his school-issued Chromebook. Three days later, he was pulled from class and brought to the school counselor's office. The district's content monitoring software had flagged his essay for self-harm language. The counselor read the entire document. Miguel was embarrassed and frustrated. "I was writing about the past," he told his parents that evening. "I'm fine now. And they read my whole essay without asking." His mother asked whether she had been notified before the meeting. She had not. His father looked up the district's device policy. It said all content on school devices could be monitored. It did not say a company would be reading it.

1. The reading discusses both potential benefits and significant concerns about keystroke monitoring in schools. Using Miguel's case, explain one benefit and one harm that this case illustrates.

2. The reading discusses the concept of self-censorship as a risk of school surveillance. Based on what happened to Miguel, explain why a student in his situation might choose to self-censor in the future, and what the reading says is lost when students do that.

Multiple Choice

1. What equity concern does the reading raise about online proctoring software?

a) Tools perform less accurately on darker-skinned faces and flag students with noisy home environments

b) Proctoring software is more expensive at schools with majority Black and Latino student populations

c) Proctoring software typically requires high-speed internet access that low-income students often lack

d) Most proctoring software is available only in English, disadvantaging multilingual students

2. What concern do critics raise about keystroke logging beyond false positives?

a) Keystroke loggers require students to pay monthly subscription fees for using monitored devices

b) The tools only work on Windows devices, creating inequality between device users

c) The software regularly deletes student work, causing academic harm

d) Students may self-censor to avoid writing about mental health, identity, or sensitive topics

3. What did a 2019 Brennan Center for Justice report find about school surveillance programs?

a) The report found no credible evidence of racial disparities in any school surveillance program

b) Schools with surveillance programs had higher graduation rates than those without

c) Many programs were implemented without evidence of effectiveness or adequate harm assessment

d) Most programs were highly effective and reduced violence in schools by 40 percent

Matching

Write the letter of the correct definition on the line next to each term.

Term	Definition
1. ___ Proctoring software	A) When individuals avoid writing or expressing themselves for fear that their words are being monitored
2. ___ FERPA	B) AI tool used to monitor students taking tests remotely, analyzing face, eyes, and behavior
3. ___ Self-censorship	C) Technology that records and monitors everything a user types on a device
4. ___ Bark/Gaggle	D) Federal law protecting student educational records, with gaps for third-party tech vendors
5. ___ Keystroke logging	E) Keystroke monitoring products that flag potential self-harm, threats, and bullying for review

Fill-in-the-Blank

1. The Lockport, New York school district became the center of a national controversy in _____ when it deployed a facial recognition system.

2. Research on school climate has found that high levels of surveillance can reduce students' sense of _____ and belonging.

3. Online proctoring software became widespread during the COVID-19 pandemic when schools shifted to _____ learning.

Short Answer

Answer each question in 2-4 complete sentences.

1. Explain the equity concerns that the reading raises about proctoring software, giving at least two specific examples.

2. What is the self-censorship risk from school surveillance, and why does the reading suggest this is particularly harmful?

3. According to the reading, what does the research say about whether school surveillance systems actually improve safety?