Companies are increasingly marketing biometric surveillance technology, like facial recognition software, as the answer to school safety concerns—and a growing number of schools in New York State are showing interest. But invasive surveillance does nothing to improve school safety and makes students feel like suspected criminals in their own classrooms.

This legislation, A 6787 (Wallace)/S 5140 (Kavanagh), will keep facial recognition and other biometric surveillance technology out of schools and require a study of the impact of this technology in schools.

The Smart Schools Bond Act provides funding to purchase technology to “improve learning and opportunity for students.” Yet instead of investing that money in the classroom for direct benefits to students, some districts are spending millions of dollars on invasive biometric surveillance and video analytics such as face, gait, voice, and fingerprint recognition software.

The state is allowing schools to spend public funds on biased, unproven, and potentially dangerous surveillance systems that infringe on student privacy and fuel the school-to-prison pipeline. This technology is often purchased without input from parents and students or any evaluation of its effectiveness or risks. School districts have also failed to create privacy policies that protect students’ most sensitive data and limit who can access it.

This legislation will ensure that biometric surveillance technology is kept out of schools and that its effects are properly studied.

A person’s biometric identifying information, like their facial characteristics, fingerprints, or voice, is highly sensitive data. It cannot be changed if there is a security breach the way a password or credit card number can be. Collecting this kind of data from children, parents, and teachers raises the risk that personally identifiable information may be inappropriately shared, sold, or hacked. School districts are ill equipped to safeguard this kind of information.

The lack of transparency and regulation around what data is collected, whether it is shared, and how it is protected as well as the invasive, dragnet nature of biometric surveillance puts our children in danger.
RACIAL BIAS

Facial recognition technology is notoriously inaccurate, especially when it comes to identifying people of color, women, and children. False positives, where the wrong student is identified and accused of misbehavior, can result in traumatic interactions with law enforcement, loss of class time, disciplinary action, and potentially a criminal record.

Biometric surveillance systems will still be biased even if they become more accurate in the coming years. For example, a system that scans faces to match them with potential threats usually relies on existing policing data like mugshot databases. The biases inherent in our criminal justice system mean that these systems will end up disproportionately hurting people of color.

SCHOOL-TO-PRISON PIPELINE

Pervasive monitoring and collection of students’ most sensitive information can turn students into perpetual suspects. This technology should not be used to track whom students associate with, to crack down on minor misbehavior, or to enforce code of conduct violations. It sets up a school climate where law enforcement tactics are the norm and punishment is a value, rather than an environment where kids can make mistakes and learn how to be accountable for their actions. As monitoring and enforcement in schools becomes more pervasive, more students could end up pushed out of the classroom for childish behavior and ensnared in the criminal justice system.

FOR MORE INFORMATION, PLEASE VISIT NYCLU.ORG