Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

2019 – 2020 Legislative Memorandum

Subject: **An Act to amend the education law, in relation to the use of biometric identifying technology**
S.5140 (Kavanagh) / A.6787 (Wallace)

Position: **SUPPORT WITH RECOMMENDATION**

Schools should be safe environments for children to learn, play, and grow. Unfortunately, a number of schools in New York state are obtaining biometric surveillance technology, like facial recognition systems, that threaten school climate and student safety. Often, these systems are purchased based solely on the sales pitch of a for-profit vendor, without critical evaluation of the technology's accuracy, security, and likely effects on the learning environment, and without adequate input from parents, teachers, and students. Pervasive monitoring and collection of students' sensitive biometric information does not make schools safer,[1] but does make students feel like perpetual suspects in their own schools.

A.6787 (Wallace)/S.5140 (Kavanagh) would prohibit schools from purchasing and using biometric surveillance technology and would mandate a comprehensive study of the risks and impacts of biometric surveillance in schools. The NYCLU strongly supports this legislation and urges its immediate passage.

Biometric surveillance, which includes face, voice, gait, and fingerprint recognition, often relies on flawed and racially-biased systems; infringes on the privacy rights of students, families, and educators; and can fuel the school-to-prison pipeline.

Facial recognition, a common form of biometric technology, is notoriously inaccurate, meaning it cannot correctly match faces to a comparison database, especially when it

[1] *Cf. The K-12 School Shooting Statistics Everyone Should Know*, CAMPUS SAFETY, Oct. 15, 2018, https://www.campussafetymagazine.com/safety/k-12-school-shooting-statistics-everyone-should-know/slideshow/5/ (demonstrating that the vast majority of school shooters are affiliated with the school and would therefore not trigger a biometric surveillance system's alert).

comes to identifying women and people of color.[2] For children, whose appearances change rapidly as they grow, biometric technologies' accuracy is even more questionable. Even false positives, where the wrong student is identified, can result in traumatic interactions with law enforcement, loss of class time, disciplinary action, and potentially a criminal record.

Biometric surveillance systems are also biased, and will continue to be so even if they become more accurate in the coming years. This is because they typically rely on law enforcement databases as comparators. For example, facial recognition systems may depend on mugshot databases, which have many more faces of people of color in them. The biases inherent in our criminal justice system[3] mean that these technologies will end up disproportionately hurting children of color – the very students who are already more likely to be punished for perceived misbehavior.

The collection and storage of biometric information is also dangerous. It requires the continual monitoring and collection of immutable characteristics, and any database of sensitive information is vulnerable to hacking and misuse. Unlike a password or credit card number, biometric data cannot be changed if there is a security breach. School districts are ill-equipped to meet the security needs of such sensitive digital information.[4]

Biometric records are covered by the federal Family Educational Rights and Privacy Act (FERPA), which prohibits the sharing of certain information in educational records without consent except in enumerated, limited circumstances,[5] and it is incumbent on schools to protect these data. Yet, some early adopters of school facial recognition systems plan to share student biometric information not only with the for-profit vendors that supply the facial recognition systems, but also with local,

---

[2] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACHINE LEARNING RES. 1, 1 – 15 (2018); *see also* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU FREE FUTURE, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28; *cf.* Paul Berger, *MTA's Initial Foray Into Facial Recognition at High Speed Is a Bust*, WALL STREET J., Apr. 7, 2019, https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000.

[3] *E.g.* Annual Stop-and-Frisk Numbers, NYCLU, https://www.nyclu.org/en/stop-and-frisk-data (last visited Apr. 11, 2019) (demonstrating that police stop, detain, frisk, and arrest Black and brown people at disproportionate rates).

[4] *E.g.* Stefanie Coyle & Naomi Dann, *We Asked for Answers on Facial Recognition in Schools. Our Questions Remain*, NYCLU, Aug. 28, 2018, https://www.nyclu.org/en/news/we-asked-answers-facial-recognition-schools-our-questions-remain.

[5] 34 C.F.R. § 99.3.

state, and federal databases.[6] These databases could include those used for immigration enforcement, which may chill some immigrant families from sending their children to school or from engaging with the school. In addition, some vendor agreements may contribute to schools violating New York Education Law §2-d, FERPA, and the Children's Online Privacy Protection Act (COPPA).

Biometric surveillance technology is an inappropriate tool for managing school safety and discipline, such as tracking who students associate with, investigating minor misbehavior, or enforcing code of conduct violations. As schools increasingly rely on law enforcement to maintain school discipline, more students are exposed to the criminal justice system than ever before. These tactics do not make schools safer. They cause damage to the school climate and can leave kids with lifelong criminal justice consequences. Ubiquitous monitoring threatens to magnify law enforcement's already serious impact on students.

Even the mere presence of biometric surveillance systems normalizes scrutiny and control, sends the message that students are viewed as potential criminals, and makes schools themselves feel more like jails.

And yet the New York State Education Department (NYSED) continues to fund school districts seeking to install these invasive systems,[7] despite issuing no additional guidance or support to help districts navigate the complexities of digital security and privacy that are implicated. New York's existing education laws and regulations do not adequately regulate the use of biometric surveillance, and schools are not seeking adequate input from parents and students; evaluating the risks of the technology or its likely effects on school climate; or adopting any privacy policies governing data retention, use, and sharing.[8]

A.6787/S.5140 would subject school biometric surveillance systems to much-needed evaluation. It would require the Commissioner of Education, in consultation with NYSED's chief privacy officer, to evaluate the privacy implications of biometric technology in schools; the reliability of the technology, and whether that reliability varies based on race, national origin, gender, age, or any other factor; whether biometric surveillance is effective for school security; whether, in what circumstances, and with whom biometric data collected by schools may be shared; the

---

[6] *E.g.* Letter from John A. Curr III, Western Regional Office Dir., & Stefanie Coyle, Educ. Couns., NYCLU, to MaryEllen Elia, N.Y. State Educ. Dep't Commissioner (Nov. 29, 2018) (on file with the author).

[7] Press Release, Gov. Cuomo, Governor Cuomo Announces $50 Million for School Technology Upgrades Through the Smart School Bond Act (Mar. 6, 2019) (https://www.governor.ny.gov/news/governor-cuomo-announces-50-million-school-technology-upgrades-through-smart-schools-bond-act).

[8] *See* Coyle & Dann, *supra* note 4.

risks of data breach; the expected maintenance costs for school biometric surveillance systems; and what notice should be provided to parents, students, and district residents when biometric surveillance is deployed in schools.[9] In short, the bill requires the Commissioner to answer the questions all schools should have answered before they began to acquire these technologies.

Critically, the bill requires the Commissioner to seek feedback from teachers, school administrators, parents, school safety experts, and student and data privacy experts.[10] While A.6787/S.5140 builds an admirable list of stakeholders, the bill should be amended to ensure that students, who would have to learn under the gaze of these biometric surveillance systems, and civil rights advocates, who are expert in the racial and gender disparities inherent in biometric surveillance systems and the databases that fuel them, have a seat at the table.

Most importantly, A.6787/S.5140 puts a moratorium on biometric surveillance in schools, prohibiting all public and nonpublic elementary and secondary schools, including charter schools, from purchasing or using biometric surveillance.

Biometric surveillance has serious privacy and educational implications for students, teachers, and parents, particularly for individuals of color and undocumented students and families. Its use in schools sends a message to students that they must be continuously monitored and, when surveillance systems are purchased instead of laptops and learning technology, that their access to educational resources is less important than their constant surveillance.

We all care about school safety, but harmful technology will not make schools safer. To do that, we need to invest in well-trained teachers, mental health professionals, guidance counselors and support staff who can build meaningful relationships with students, pay attention when things are going wrong, and create a culture of trust and accountability. A.6787/S.5140 will stop an expensive "quick fix" panacea that promises more harm than good.

The NYCLU strongly supports A.6787/S.5140, urges that it be amended to include input from students and civil rights advocates, and calls for its swift passage.

[9] A.6787 § 2, 2019-2020 Reg. Sess. (N.Y. 2019).
[10] A.6787 § 3, 2019-2020 Reg. Sess. (N.Y. 2019).