



Legislative Affairs
125 Broad Street, 19th Floor
New York, NY 10004
212-607-3300
www.nyclu.org

2025 – 2026 Legislative Memorandum

Subject: An Act to amend the state technology law, in relation to banning the use of biometric identifying technology in schools
S.3827 (Hoylman-Sigal) / A.6720 (Simone)

Position: SUPPORT

Schools should be safe environments for young people to learn, play, and grow. As New York has started to recognize, subjecting students to invasive biometric surveillance technology is directly at odds with that goal.

Following a legislatively-mandated moratorium on the use of biometric identifying technologies in schools, the New York State Office of Information Technology Services (OITS) conducted an extensive study on the use of the technology in schools, ultimately concluding that “the risks of the use of [facial recognition] in an educational setting may outweigh the benefits.”¹ The Commissioner of Education responded to this report by creating regulations that banned the use of facial recognition in schools. S.3827 (Hoylman-Sigal) / A.6720 (Simone) would codify and expand upon this rule, prohibiting public, private, and charter elementary and secondary schools in New York from purchasing or using biometric surveillance technology. 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; fuels the school-to-prison pipeline; and has serious educational implications for students of color and undocumented students and families.

¹ *Biometric Identifying Technology in Schools*, NEW YORK STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES, Aug. 7, 2023, <https://its.ny.gov/system/files/documents/2023/08/biometrics-report-final-2023.pdf>.

Facial recognition, a common form of biometric technology, is notoriously inaccurate, meaning it cannot correctly match faces to a comparison database, especially when it 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.³ Even false positives, where students are misidentified, can result in traumatic interactions with law enforcement and criminal legal consequences, on top of the loss of valuable learning time and alienation from school. What's more, because biometric surveillance systems typically rely on law enforcement databases as comparators, these systems inevitably mirror the racial disparities of our criminal legal system⁴ and, in the schools context, disproportionately target and harm children of color.

These systems, by design, require the continual monitoring and collection of sensitive immutable characteristics, meaning any database of biometric information is vulnerable to hacking and misuse.⁵ Unlike a password or credit card number, biometric data cannot be changed in the event of a security breach. As has been shown time and time again, school districts are ill-equipped to meet the security needs of such sensitive digital information.⁶ As the NYCLU has found, there is also the danger that districts share student biometric information with local, state, and

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 Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPT OF COMMERCE, Nov. 2018, <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>; Patricia Scanlon, *Voice Assistants Don't Work for Kids: The Problem with Speech Recognition in the Classroom*, TECHCRUNCH, Sept. 9, 2020, <https://techcrunch.com/2020/09/09/voice-assistants-dont-work-for-kids-the-problem-with-speech-recognition-in-the-classroom>.

⁴ E.g. Annual Stop-and-Frisk Numbers, NYCLU, <https://www.nyclu.org/en/stop-and-frisk-data> (last visited Dec. 9, 2025) (demonstrating that police stop, detain, frisk, and arrest Black and brown people at disproportionate rates).

⁵ *How Biometrics Are Attacked, Biometric Recognition and Authentication Systems*, NATIONAL CYBER SECURITY CENTRE, Jan. 24, 2019, <https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked>; Rachael Altman, *Cybersecurity Concerns Escalate in the Education Industry*, G2, Nov. 2, 2021, <https://www.g2.com/articles/cybersecurity-concerns-in-the-education-industry>.

⁶ 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>.

federal databases,⁷ in violation of state and federal education and privacy laws.⁸ In this way, biometric surveillance technology emboldens the reach of law enforcement into everyday school matters, such as tracking who students associate with and investigating student behavior at a scale previously unheard of. As students continue to name, the mere presence of biometric surveillance systems sends the message that access to resources for learning is less important than their constant surveillance, and makes schools look and feel more like jails.

S.3827 / A.6720 addresses these concerns by banning biometric surveillance in schools, prohibiting all public and nonpublic elementary and secondary schools, including charter schools, from purchasing or using biometric surveillance.⁹ This legislation will protect students and families from dangerous, misguided attempts to harden schools, and instead make way for real safety strategies and robustly resourced schools that center relationships, care, and opportunities to learn.

The NYCLU strongly supports S.3827 / A.6720 and calls for its swift passage.

⁷ *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).

⁸ New York Education Law §2-d; Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. §99.31; Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501.

⁹ Except for fingerprint identification for prospective employees where written consent is given.