SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

MEMORANDUM OF SUPPORT

Date: April 1, 2024
To: All Assembly Members, New York State Assembly; All Senators, New York State Senate; Governor Kathy Hochul
From: The Surveillance Technology Oversight Project (S.T.O.P)

Re: S.T.O.P. Memorandum in Support of School Biometrics Ban (S.7944 Hoylman-Sigal/A.8853 Wallace)

S.T.O.P. is a community-based civil rights group that litigates and advocates against discriminatory surveillance. S.T.O.P. works to abolish local governments' systems of mass surveillance. Our work highlights the discriminatory impact of surveillance on Muslim Americans, immigrants, the LGBTQ+ community, indigenous peoples, and communities of color, particularly the unique trauma of anti-Black policing. We craft policies that balance new technologies and age-old rights.

S.T.O.P. emphatically supports the School Biometrics Ban (S.7944/A.8853). Because of its documented biases and the dangers it poses to students, particularly students of color, LGBTQ+ students, immigrant students, and students with disabilities, facial recognition has no place in schools. This bill codifies the existing regulatory ban on biometrics in schools. Specifically, it forbids public, private, and charter elementary and secondary schools in New York from purchasing or utilizing biometric identifying technology, except for fingerprint identification for prospective employees where written consent is given.

The New York State Office of Information Technology Services (ITS) conducted an extensive study on use of biometric identifying technology in schools and ultimately concluded that "the risks of the use of [facial recognition] in an educational setting may outweigh the benefits."[1] In September 2023, the Commissioner of Education responded to this report by creating regulations that banned the use of facial recognition and other biometrics in schools. S.7944/A.8853 would simply codify this ban, ensuring this protection for students lasts.

One of the biggest risks of facial recognition is the bias baked into the artificial intelligence on which it operates. Facial recognition systems may be up to 99 percent accurate on white men,[2] but can be wrong more than one-in-three times for women of color.[3] And since these systems are often programmed to recognize only two genders, they leave transgender and nonbinary individuals invisible

[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.
[2] Steve Lohr, *Facial Recognition is Accurate, if You're a White Guy*, NEW YORK TIMES, Feb. 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.
[3] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," in *Conference on Fairness, Accountability and Transparency*, pp. 77-91, PMLR, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

and subject to misidentification.[4] Concerningly, facial recognition technology has even higher inaccuracy rates when used on students.[5] Voice recognition software, another widely known biometric surveillance tool, echoes this pattern of poor accuracy for those who are nonwhite, non-male,[6] or young,[7] which underlies the futility of employing these faulty tools in New York classrooms.

Collecting and storing biometric data in schools also threatens to expose children to unnecessary and preventable privacy and safety risks. This data is vulnerable to a variety of security threats,[8] including hacking, data breaches and insider attacks, and schools tend to have inadequate cybersecurity practices,[9] putting children at great risk of being tracked and targeted by malicious actors.[10] Additionally, one study found that CCTV systems in U.K. secondary schools led many students to suppress their expressions of individuality and alter their behavior.[11] There is also the danger that districts could send the biometric information captured by facial recognition technology to law enforcement or immigration authorities, like ICE, putting undocumented students and undocumented families of American children at risk. Normalizing biometric surveillance will bring about a bleak future for kids at schools across the state.

Importantly, surveilling students using facial recognition will not make students safer. The ITS study emphasized the flawed reasoning behind this safety argument, finding no evidence that facial recognition has ever prevented violence in a school environment.[12] In fact, since the majority of school shootings are committed by current students or alumni of the school in question, facial recognition systems would likely not flag these faces as suspicious and therefore would be useless in protecting students.[13] And even if the technology were to flag a real potential perpetrator of violence, given

---

[4] Rachel Metz, *AI Software Defines People as Male or Female. That's A Problem*, CNN BUSINESS, Nov. 21, 2019, https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html.
[5] Patrick Grother, Mei Ngan, and Kayee Hanaoka, Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE, Nov. 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.
[6] Rachael Tatman and Conner Kasten, "Effects of Talker Dialect, Gender & Race on Accuracy of Bing Speech and YouTube Automatic Captions," in *Interspeech*, pp. 934-938, 2017, https://www.isca-speech.org/archive_v0/Interspeech_2017/pdfs/1746.PDF.
[7] 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.
[8] *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.
[9] Rachael Altman, *Cybersecurity Concerns Escalate in the Education Industry*, G2, Nov. 2, 2021, https://www.g2.com/articles/cybersecurity-concerns-in-the-education-industry.
[10] Benjamin Herold, *FBI Raises Alarm on Education Technology and Security of Students*, EDWEEK, Sept. 18, 2018, https://www.edweek.org/leadership/fbi-raises-alarm-on-education-technology-and-security-of-students/2018/09
[11] Claire Galligan, Hannah Rosenfeld, Molly Kleinman, and Shobita Parthasarathy, *Cameras in the Classroom: Facial Recognition Technology in Schools*, U. MICH. SCIENCE, TECHNOLOGY, AND PUBLIC POLICY PROGRAM, 2020, at 10, https://stpp.fordschool.umich.edu/sites/stpp/files/uploads/file-assets/cameras_in_the_classroom_full_report.pdf.
[12] *Biometric Identifying Technology in Schools*, NEW YORK STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES, Aug. 7, 2023, at 17, https://its.ny.gov/system/files/documents/2023/08/biometrics-report-final-2023.pdf.
[13] Ava Kofman, *Face Recognition Is Now Being Used in Schools, But It Won't Stop Mass Shootings*, INTERCEPT, May 30, 2018, https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings.

the speed at which most school shootings usually come to an end,[14] it is unlikely that law enforcement would be notified and able to arrive to the scene in time to prevent such horrendous acts.

Banning facial recognition in schools is necessary to protect New York kids from racially biased, ineffective, unsecure, and dangerous tech. We urge the legislature to pass, and the Governor to sign, the School Biometrics Ban (S.7944/A.8853).

[14] John Woodrow Cox and Steven Rich, *Scarred by School Shootings*, WASH. POST, March 25, 2018, https://www.washingtonpost.com/graphics/2018/local/us-school-shootings-history/?noredirect=on&utm_term=.3074101be628.