1400 Eye Street NW, Suite 450, Washington, DC 20005 | 202-768-8950 | fpf.org

New York State Assembly
New York State Capitol
Washington Ave and State St
Albany, NY 12224

June 14, 2019

Dear Speaker Heastie, Education Committee Chair Benedetto and Assemblymember Wallace,

As the New York State Assembly considers revisions to New York's state education laws regarding biometric identifying technology, we write to support a well-crafted moratorium on facial recognition systems for security uses in public schools. At the same time, we would like to caution against overly broad bans or language that might have unintended consequences on other security programs, including some that may include biometric technology.

We recommend:

- A targeted moratorium specifically focused on pausing the use of facial recognition systems for security purposes at public school facilities, rather than banning the use of all biometric technology prior to July 2022;
- Permitting the continued operation of existing biometrics systems that do not rely on facial recognition, such as fingerprint and palm-print systems, and requiring a review of these systems; and
- Analysis and reporting regarding the risks and benefits of biometric technology in schools. The report should include recommendations concerning both 1) the appropriate notice regarding the use of facial recognition systems; and 2) the appropriate level of consent applicable to such systems, if facial recognition technology is approved for future use.

The Future of Privacy Forum is a nonprofit organization focused on consumer privacy issues, including issues affecting students, parents, teachers, and others with a stake in protecting education data. We primarily help key stakeholders find actionable solutions to the privacy concerns resulting from the speed of technological development. FPF's education privacy project has worked for five years to ensure student privacy while supporting educational technology and innovation that can help students succeed.

FPF maintains FERPAlSherpa, a website compiling education privacy resources for parents, schools, edtech companies, and other stakeholders; we run a student privacy working group for districts and state privacy staffers representing 45 states; and we are a co-founder of the Student Privacy Pledge, a voluntary, legally enforceable code of conduct for edtech companies. We have testified before Congress and the Federal School Safety Commission on education privacy, and the Federal Trade Commission and U.S. Department of Education invited us to present on student privacy state laws at their 2017 workshop on the intersection between the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA).

We appreciate your important work on student privacy. As we all seek to provide appropriate protections for student data, we should ensure that schools can maximize the benefits of technology for students and their learning outcomes. We support a moratorium to allow time for comprehensive study of the impact of facial recognition systems on school campuses. Our analysis of the risks and benefits of facial recognition systems suggests that an evidence-based review of widespread use of these systems in schools will likely find that the systems do not offer sufficient benefits when used for security purposes at public schools. Although the desire to provide the highest levels of security and protection for students and school personnel is well-intentioned, it is unclear that facial recognition systems will actually make schools safer. Particularly in light of the costs of purchase, implementation, training, and maintenance, we believe the study is unlikely to find sufficient value or benefit in these systems to justify their risks and privacy impacts.

Schools may also face backlash from parents and staff who don't want to be involved in such a system. For example, some parents who volunteer at school may wish to opt out of having their biometric information

collected and stored. Although privacy best practices would require provision of an alternate method, any barrier to entry may decrease people's willingness to volunteer or come to the school at all. For similar reasons, employees may also resist. Schools would thus incur additional costs to create alternatives for individuals who do not want to take part in a facial recognition system.

While we support a moratorium on this technology, some provisions of the draft law contain broad language that may lead to unintended consequences. Facial recognition systems for campus security have triggered the immediate concerns, and that should be the moratorium's target. Schools may implement facial categorization technologies in other ways that, if banned outright, would prevent or compromise current services to students. For example, schools may currently use biometric software that does not identify individuals but measures facial expressions, voice data, or gait analysis in order to help students in special education, occupational therapy, and physical therapy programs. If the ban applies broadly to all biometrics in all cases, it could unintentionally eliminate these services and programs.

Likewise, some school systems in New York have already purchased and implemented biometric systems based on fingerprints and palm prints for lunch-line efficiencies, attendance reporting, and other administrative functions. These systems are widespread throughout the country and have not typically presented high risk factors for student privacy. Allowing these school districts to continue using these systems would prevent unnecessary costs of reverting to less-reliable technology, unless or until any risks are identified. Excessively broad language concerning biometric collection or use might even compromise the current practice of collecting the fingerprints of staff and other employees at public schools in order to run background checks, an outcome that would actually decrease student safety.

Instituting a moratorium on facial recognition technology in schools, while permitting continued operation of other existing biometric programs would mitigate privacy risks while creating time for the state to review the risks and benefits of biometric programs for students, teachers, parents, and others. The study should, of course, consider all aspects of biometrics use and make appropriate recommendations. By allowing existing programs to continue in the interim, schools could gradually make necessary changes without negatively impacting students or services.

Finally, if the study does find appropriate uses or justifications for facial recognition systems, we recommend that the current requirement to provide appropriate notice to those affected be expanded to require appropriate consent by school employees, students, visitors, and others who might be impacted. Establishing an express consent requirement and/or options to opt out are important for protecting individual privacy.

Thank you very much for your advocacy and support for the strong protection of student data. Please feel free to contact us if you have any questions or would like additional information.

Sincerely,

Brenda Leong

Senior Counsel, Biometric Privacy, Future of Privacy Forum

Amelia Vance

Director of Education Privacy, Future of Privacy Forum