GERALD R. **FORD SCHOOL** OF PUBLIC POLICY
UNIVERSITY OF MICHIGAN

January 15, 2022

Dr. Eric Lander
Director
Office of Science and Technology Policy
1600 Pennsylvania Ave NW
Washington, DC 20500

Re: Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Dear Dr. Lander,

Thank you for the opportunity to comment on the question of regulating AI-enabled biometric technologies. I am writing in my capacity as Director of the Science, Technology, and Public Policy (STPP) program. The STPP Program is a research center based in the Gerald R. Ford School of Public Policy at the University of Michigan in Ann Arbor. Our mission is to address urgent questions at the intersection of science, technology, policy, and society, with the aim of producing more just and equitable science and technology policies. We bring a rigorous interdisciplinary lens to understanding these concerns, and translating them to policymakers, engineers, scientists, and civil society.

STPP's research team recently conducted an investigation of the potential implications of using facial recognition (FR) technology in schools, and our findings are that FR brings many harms with very few rewards. Some of these harms have already been realized (See https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition-technology-schools for the full report and additional documentation).

On this basis of this research, we strongly recommend that facial recognition be banned in school settings, on the basis of the far-reaching harm it is capable of; however, should schools proceed with its implementation, we have policy recommendations regarding its development, deployment, and regulation.

Exhibited and potential harms of facial recognition in schools

FR perpetuates racism and other forms of bias. Using FR technology in schools is likely to amplify, institutionalize, and potentially weaponize existing racial biases, resulting in disproportionate surveillance and humiliation of marginalized students. It is likely to mimic the impacts of school resource officers (SROs), stop-and-frisk policies, and airport security. All of these interventions purport to be objective and neutral systems, but in practice they reflect the structural and systemic biases of the societies around them. All of these practices have had racist outcomes due to the users of the systems disproportionately targeting people of color.

These cases have also revealed that technologies that target subjects along racist lines result in negative psychological and social outcomes for these subjects, in this case school children. The use of metal detectors in schools decreases students' sense of safety, for example. Because FR is a similar surveillance technology that has potential to amplify user biases, it is likely that FR systems in schools will disproportionately target students of color, harming them psychologically and socially. Finally, FR algorithms consistently show higher error rates for people of color, with white male subjects consistently enjoying the highest accuracy rates. In sum, students of color are more likely to be targeted by FR surveillance and more likely to be misidentified by FR. multiplying the negative impacts of the tool.

FR brings state surveillance into the classroom. Implementing FR in schools will normalize the experience of being constantly surveilled, starting at a young age. Furthermore, once implemented, it will be hard to control how administrators use FR and for what purposes. The case of closed- circuit television (CCTV) reveals how surveillance technologies can undergo mission creep: CCTV systems in secondary schools in the United Kingdom (UK) were originally instituted for school security, but in practice became most often used for monitoring student behavior. It is likely that FR will also undergo mission creep as administrators expand the usage of the technology outside of what was originally defined. The normalization of surveillance will result in negative psychological and social effects for students. Several cases demonstrate that surveillance technologies make subjects feel powerless, as they feel that they are always being watched. This is likely to be replicated with FR in schools. Finally, limited data protections in the face of widespread surveillance puts subjects' privacy at greater risk, and this would also be a significant risk for children in schools with FR systems.

FR punishes nonconformity. FR in schools is also likely to discipline young people in unexpected ways, by narrowing the definition of the "acceptable student" and punishing those who fall outside that definition. For example, CCTV systems in UK secondary schools led many students to reclassify their expressions of individuality and alter their behavior. Students reported that their style of dress seemed to influence how likely they were to be disciplined, meaning that non-criminal expressions of individuality could warrant punishment for students. Students also reported avoiding certain areas where they were likely to be surveilled, and behaving in ways less likely to draw attention. Additionally, FR is likely to further marginalize minority groups, as India's Aadhaar system did. Aadhaar excludes citizens who have damaged fingerprints or eyes, which disproportionately impacts marginalized people including manual laborers and leprosy patients. This often means that these individuals are unable to access food rations or welfare, thus harming groups that were already disadvantaged.

FR in schools is likely to similarly exclude students, given that students of color, immigrant students, students with disabilities, gender non-conforming students, and low-income students all are likely to have lower accuracy and higher flag rates both automatically due to the design of FR and by human administrators of the system. Depending on how the school is using FR, this could result in already marginalized students being incorrectly marked absent for class, prevented from checking out library books or paying for lunch. FR systems in schools are poised to privilege some students and exclude and punish others based on expressions of individuality and characteristics outside of their control.

FR companies profit from children's personal data. FR in schools is likely to generate new data on students and create new markets in commodifying student data. Previous experience with similar data-generating technologies suggests that providers of these technologies will seek to commodify data collected, creating concerns about ownership, consent, value, and market exploitation. Providers may even offer FR services at no cost in exchange for the ability to collect and monetize the data. There is limited legal and policy clarity about whether citizens own their data. Most cases suggest that though citizens do not have ownership over their biometric data, they have a right to full, informed consent. This framing has been reinforced by the dozens of biobanks that scientists and governments have created over the last few decades, which assert ownership over human DNA samples and other specimens, along with their resulting data. However, given the design of FR tools, which are meant to be applied broadly to any and all faces that move through or near a given system, advance consent may be difficult or impossible to obtain. Further, there is concern that making biometric data collection a routine part of school life, especially without any explicit discussion about where and how to release this data, teaches students that it is normal and unremarkable to give away biometric data and have it used to track your location, purchases, and activities. Altogether, our analysis indicates that the institution of FR in schools threatens students' data privacy and security, will result in data collection without consent, and will create a culture of permissiveness regarding data collection, leaving children particularly vulnerable to unauthorized use of their personal information.

FR is inaccurate. Establishing and maintaining accuracy in FR systems in schools will likely be very difficult. FR is neither as accurate nor as unbiased as developers claim it will be, meaning that users likely will have misaligned expectations of the technology, and be willing to entrust it with work for which it is fundamentally unsuited. In addition, while FR is seductive because the automated face-matching process seems to side step individual biases, humans and our judgment are involved at every step. For example, just as humans make final matching determinations with closed- circuit television (CCTV) and fingerprinting, so will they with FR technology. As we have seen in those cases, though these technologies are often automatically accepted by users as objective and highly accurate, they are actually influenced by human bias and error. Additionally, the lack of regulation surrounding the breathalyzer suggests that a similar lack of regulation of FR in schools could result in errors in the calibration of the technology and in how results are interpreted. Some may argue that the way to address these problems is through enhanced accuracy. But perfect accuracy would potentially make FR in schools even more damaging in the ways described above.

Further, cases of similar technologies illuminate how excitement over a technological fix can lead to entrenchment, even if the tool is not necessarily accurate. These cases also show the sustained resources and training needed to maintain accuracy, the difficulty of assessing accuracy for low-probability events, the problems with having courts as the ultimate arbiters of accuracy, the racial bias that is embedded in surveillance technologies, and the challenge of having local officials determine accuracy among heterogeneous products. Overall, it is difficult to imagine how FR systems will establish and maintain a high level of accuracy in schools.

Recommended governance for facial recognition in schools

Owing to the overwhelmingly adverse effects observed and anticipated when implementing and using facial recognition in schools, **we strongly recommend that FR technology be banned in schools**. However, recognizing that such technology is likely to be implemented, accepted, and eventually pervasive, we have outlined recommendations that would serve to mitigate the harmful effects of FR and allow for fair, safe, and ethical use whilst protecting the privacy and mental and social well-being of vulnerable student bodies. Should FR be introduced into schools, we urge caution and extensive deliberation to ascertain whether such investments are ultimately beneficial. Public input, especially from the most vulnerable stakeholders – students of color, the disabled, gender-nonconforming individuals, and immigrants – must be considered and factored into decision-making, and investment based on supposed technological accuracy must be superseded by considerations of the technology's impacts on social, ethical, racial, and economic dimensions inherent in school systems. As existing laws and policies are insufficient to manage the novelty, emergence, and potential scope and power of FR, clear and robust regulations are necessary to protect students; laws must also allow for periodic revision and opportunities for regulatory change, as FR technology evolves and consequences become clear, and as new challenges arise.

Policy Recommendations: National Level

1. Implement a **nationwide moratorium** on all uses of FR technology in schools. The moratorium should last as long as necessary for the national advisory committee to complete its work and for the **recommended regulatory system** to be fully and safely implemented on a national level. We anticipate that this process, and hence this moratorium, will last **5 years**.
2. Enact comprehensive data privacy and security laws if they are not already in place.
3. Convene a national advisory committee to investigate FR and its expected implications, and to recommend a regulatory framework to govern this technology. The national advisory committee should be **diverse in terms of both demographic and professional expertise**. This committee should include experts in: technical dimensions of FR (e.g., data scientists); privacy, security, and civil liberties laws; social and ethical dimensions of technology; race

and gender in education; and child psychology. The committee should also include those involved in kindergarten through high school (K-12) operations, including teachers, school administrators, superintendents, high school students, and parents or guardians of elementary and middle school students. Government officials from relevant agencies (e.g., in the US, the Department of Education and Federal Communications Commission) should be invited to participate in the committee as ex officio members; they could provide important insight into the regulatory options available. Representatives of FR companies should be invited to testify periodically in front of the committee, so that their perspectives can be considered in the regulatory process. Finally, efforts should be made to elicit community perspectives, ideally through **deliberative democratic efforts**.

4. Create **additional oversight mechanisms** for the technical dimensions of FR

Policy Recommendations: State Level

If a state allows FR in schools, it should create programs and policies that fill in any gaps left by national policy as well as establishing new infrastructure for the oversight and management of district-level FR use.

5. **Convene a state-level expert advisory committee to provide guidance to schools and school districts**, if a regulatory framework is not created at the national level. There should be a moratorium on adopting FR in schools until this guidance has been provided.
6. **Establish technology offices**, perhaps within state departments of education, to help schools navigate the technical, social, ethical, and racial challenges of using FR and other emerging educational technologies. These offices should also **provide resources and oversight** to ensure that school and district staff are properly trained to use FR technology in a way that is consistent with state laws.

Policy Recommendations: School and District Level

Schools and school districts are directly responsible for the installation and operation of FR, and for any disciplinary action that follows from identification, so they are responsible for most of the oversight actions.

7. If any alternative measures are available to meet the intended goals, do not purchase or use FR.
8. Perform a thorough evaluation of FR, including ethical implications, before purchasing it. This is even more crucial in the absence of national regulations or state-level guidance.
9. Develop a plan for implementing the technology before using it.
10. Do not purchase FR systems that use student social media accounts to improve the technology.
11. Do not use FR technology to police student behavior.
12. Delete student data at the end of each academic year or when the student graduates or leaves the district, whichever comes first.
13. Employ at least one person dedicated to managing and maintaining the FR technology in each school.

14. Provide regular, age appropriate guidance to parents, guardians, and students that includes information about why the school has deployed FR, how it will be used, how data will be managed, and what protections are in place to ensure accuracy and equity

15. Establish a pilot period and re-evaluation process before full-scale implementation of the technology.

In conclusion, we appreciate OSTP's efforts to investigate biometric technologies. We believe the evidence fully supports increased regulation of these technologies to protect Americans from their potential harms. Thank you in advance for your consideration of our comments.

Sincerely,

Shobita Parthasarathy

Shobita Parthasarathy, Ph.D.
Professor
Director, Science, Technology, and Public Policy program
Gerald R. Ford School of Public Policy
University of Michigan
shobita@umich.edu
https://stpp.fordschool.umich.edu/