EXECUTIVE SUMMARY

Cameras in the Classroom

Facial Recognition Technology in Schools

Claire Galligan
Hannah Rosenfeld
Molly Kleinman
Shobita Parthasarathy

GERALD R. FORD SCHOOL OF PUBLIC POLICY
SCIENCE, TECHNOLOGY, AND PUBLIC POLICY
UNIVERSITY OF MICHIGAN

TECHNOLOGY ASSESSMENT PROJECT REPORT

About the Authors

Claire Galligan graduated Phi Beta Kappa from the University of Michigan in May 2020 with a BA in Public Policy and a minor in Economics. Her research and policy interests include technology, trade and economics, healthcare, and foreign policy. She has held internships in Congressman Dan Kildee's (MI-05) Washington, DC office and on TD Bank's Government Relations team. During her time at the University of Michigan, she worked as the President of the Michigan Foreign Policy Council, an on-campus foreign policy think tank, where she helped produce a biannual journal of original student research and pioneered a professional development mentorship program where students were paired with professional researchers at the Brookings Institution to receive research and writing advice. Claire will soon be an Associate with Kaufman Hall & Associates on their healthcare consulting team (based in Chicago).

Hannah Rosenfeld is a Master of Public Policy student at University of Michigan, where she is in the Science, Technology, and Public Policy and Diversity, Equity, and Inclusion graduate certificate programs. She holds a BA in Biology from University of Virginia. Hannah worked in the tech and tech regulation industry for over 7 years on education technology, medical devices, and personal security, including at Luidia and Oculogica. In addition to experience in research, regulatory compliance, and program and technology evaluation, she has developed diagnostic tools that leverage machine learning and computer vision. She has also worked with university officials and security teams around the country to develop responsive emergency technology. She is on the Foretell Ambassador Board for technology forecasting with Georgetown's Center for Security and Emerging Technology (CSET) and formerly led the New York City chapter of the LGBTQ+ non-profit Out in Tech before becoming the Head of Diversity, Inclusion, and Belongingness for the international organization.

Molly Kleinman is the Program Manager of the Science, Technology, and Public Policy program at the University of Michigan, and a lecturer at the University of Michigan School of Education. She studies higher education policy, access to information, and faculty experiences with technology. Molly spent several years as an academic librarian at the University of Michigan, and served as program manager for clinical and basic science education at the University of Michigan Medical School. Molly received her Ph.D. in Higher Education Policy from the University of Michigan Center for the Study of Higher and Postsecondary Education, with a certificate in Science, Technology, and Public Policy, her MS in

Information from the University of Michigan School of Information, and her BA in English and Gender Studies from Bryn Mawr College.

Shobita Parthasarathy

is Professor of Public Policy and Women's Studies, and Director of the Science, Technology, and Public Policy Program, at the University of Michigan. She conducts research on the ethical, social, and equity dimensions of emerging science and technology and associated policies, as well as the politics of evidence and expertise in policymaking, in comparative and international perspective. She is the author of multiple articles and two books: *Building Genetic Medicine: Breast Cancer, Technology, and the Comparative Politics of Health Care* (MIT Press, 2007) and *Patent Politics: Life Forms, Markets, and the Public Interest in the United States and Europe* (University of Chicago Press, 2017). She has advised policymakers in the United States and around the world how to regulate emerging science and technology in the public interest. She is a non-resident fellow of the Center for Democracy and Technology and sits on the advisory board for the Community Technology Collective. She writes frequently for the public and co-hosts *The Received Wisdom* podcast, on the relationships between science, technology, policy, and society.

About the Science, Technology, and Public Policy Program

The University of Michigan's **Science, Technology, and Public Policy (STPP) program** is a unique research, education, and policy engagement center concerned with cutting-edge questions that arise at the intersection of science, technology, policy, and society. Housed in the Ford School of Public Policy, STPP has a vibrant graduate certificate program, postdoctoral fellowship program, public and policy engagement activities, and a lecture series that brings to campus experts in science and technology policy from around the world. Our affiliated faculty do research and influence policy on a variety of topics, from national security to energy.

PDF: Click to return to top

Executive Summary

Facial recognition (FR) technology was long considered science fiction, but it is now part of everyday life for people all over the world. FR systems identify or verify an individual's identity based on a digitized image alone, and are commonly used for identity verification, security, and surveillance in a variety of settings including law enforcement, commerce, and transportation. Schools have also begun to use it to track students and visitors for a range of uses, from automating attendance to school security. FR can be used to identify people in photos, videos, and in real time, and is usually framed as more efficient and accurate than other forms of identity verification. However, a growing body of evidence suggests that it will erode individual privacy and disproportionately burden people of color, women, people with disabilities, and trans and gender non-conforming people.

In this report, we focus on the use of FR in schools because it is not yet widespread and because it will impact particularly vulnerable populations. We analyze FR's implications using an analogical case comparison method. Through an iterative process, we developed historical case studies of similar technologies, and analyzed their social, economic, and political impacts, and the moral questions that they raised. This method enables us to anticipate the consequences of using FR in schools; our analysis reveals that FR will likely have five types of implications: exacerbating racism, normalizing surveillance and eroding privacy, narrowing the definition of the "acceptable" student, commodifying data, and institutionalizing inaccuracy. Because FR is automated, it will extend these effects to more students than any manual system could.

Schools have begun to use facial recognition to track students and visitors for a range of uses, from automating attendance to school security.

On the basis of this analysis,

we strongly recommend that use of FR be banned in schools.

However, we have offered some recommendations for its development, deployment, and regulation if schools proceed to use the technology.

PDF: Click to return to top

The Implications of FR in Schools

Exacerbating Racism

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. For example, though predictive policing is supposed to remove the bias of individual officers, in practice its deployment in predominantly Black and brown neighborhoods, its training data, and its algorithms all serve to reproduce bias on a systemic level and disproportionately harm Black and brown people, to such an extent that several cities have recently discontinued its use. These cases have also revealed that technologies that target subjects along racist lines result in negative psychological and social outcomes for these subjects. 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.

Normalizing Surveillance

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 analogical 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. Considering

Burst (CC-0)

PDF: Click to return to top

FR's similarities to CCTV in terms of form and function, 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. CCTV, as well as the cases of fingerprinting in schools and India's Aadhaar system, 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. This was the case with India's Aadhaar system, where citizens' biometric data has been subject to security breaches, and would also be a significant risk in school FR systems.

Defining the Acceptable Student

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. In these ways, analogies to FR indicate that it is likely to define the "acceptable" student and discipline those who fall outside of that definition. 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.

The Gender Spectrum Collection, CC BY-NC-ND 4.0

PDF: Click to return to top

Commodifying 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 young people particularly vulnerable to unauthorized use of their personal information.

Institutionalizing Inaccuracy

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

FR is neither as accurate nor as unbiased as developers claim it will be...But perfect accuracy would potentially make FR in schools even more damaging.

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, the cases of CCTV and airport security illuminate how excitement over a technological fix can lead to entrenchment, even if the tool is not necessarily accurate. Just as CCTV rarely deters crime in the UK despite being widely implemented, it is likely that FR, which is similar to CCTV in form and function, could similarly become entrenched despite inaccuracies. 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.

National and International Policy Landscape

At present, there are no national laws dedicated to regulating FR anywhere in the world. In fact, quite the opposite: many countries are expanding their use of the technology without any regulatory policies in place (**Map A, see report supplement**). There is, however, some policy activity, which we have divided into five types. A handful of US states and localities have implemented **bans or moratoria**, often on particular uses of FR. More common are **consent and notification** and **data security** policies, which are not specific to FR but regulate some of the data generated and used. Consent and notification policies cover the data collection process, creating requirements about obtaining consent and notifying individuals, while data security policies focus on how to protect data once it is already collected such as with encryption standards or local storage mandates. These policies often go hand in hand, such as in the European Union's (EU) General Data Protection Regulation (GDPR). India, Kenya, and a handful of US states have passed or are seriously considering similar policies. We also see limited efforts to **tailor use**, such as in Detroit's Project Greenlight which is used for a handful of law enforcement purposes. Finally, some have proposed **oversight, reporting, and standard-setting** policies which would mandate accuracy standards and reporting requirements for FR systems. None of these have been implemented.

Recommendations

Based on our analysis, **we strongly recommend that the technology be banned for use in schools.** However, if schools and departments of education decide to proceed with FR, then they must do so cautiously, after extensive expert deliberation and public participation (particularly among vulnerable groups), and with a clear regulatory framework that considers the social, ethical, racial, and economic dimensions of the technology—far more than the technology's accuracy. Existing laws and policies are simply insufficient to manage this powerful technology, which could have impacts long after the children involved leave school. Any laws or policies governing FR must also provide multiple opportunities for review and change, as the technology's consequences become clearer.

Based on our analysis, we strongly recommend that the technology be banned for use in schools.

While we strongly recommend a ban, below we provide policy recommendations if schools decide it is absolutely necessary to implement the technology. In addition, in the **full report** (Appendices A and B) we have provided stakeholders (e.g., parents/guardians, students, and school administrators) with sample questions to help them evaluate the technology.

PDF: Click to return to top

National Level

RECOMMENDATIONS

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.

PDF: Click to return to top

State Level

RECOMMENDATIONS

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.

School and School District Level

RECOMMENDATIONS

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.

PDF: Click to return to top

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.**

What to Ask

To assist administrators, parents, guardians and students evaluate specific FR use in their schools, we offer sample questions in Appendices A and B of the **complete report.**

VIEW THE FULL REPORT

myumi.ch/schoolfrban

If you would like additional information about this report, the Technology Assessment Project, or University of Michigan's Science, Technology, and Public Policy Program, you can contact us at **stpp@umich.edu** or **stpp.fordschool.umich.edu**.

GERALD R. FORD SCHOOL OF PUBLIC POLICY
SCIENCE, TECHNOLOGY, AND PUBLIC POLICY
UNIVERSITY OF MICHIGAN

Technology Assessment Project
Science, Technology, and Public Policy Program
Gerald R. Ford School of Public Policy
University of Michigan
735 S. State Street
Ann Arbor, MI 48109

(734) 764-0453
stpp.fordschool.umich.edu
stpp@umich.edu