

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

Contents

About the Authors	5	Exacerbating Racism	30
		FR Accuracy Varies by Race	31
About the Science, Technology, and Public Policy Program	6	Disproportionately Targeting People of Color	31
		Adverse Psychological and Social Impacts	35
Acronyms	7	Normalizing Surveillance	38
Executive Summary	8	Technology Expanding the Reach of Surveillance	39
The Implications of FR in Schools	9	Students Feel Powerless	41
National and International Policy Landscape	12	Defining the Acceptable Student	43
Recommendations	13	Reclassifying Expressions of Individuality	44
Introduction	17	Further Marginalizing Vulnerable Groups	44
How Does the Technology Work?	17	Altering Behaviors to Avoid Surveillance	45
FR's History	19		
The FR Landscape Today	20		
School Security and FR	22		
Analogical Case Comparison: Our Analytic Approach	23		
Analogical Case Studies	26		
Overview of the Implications	28		

Creating New Commodities and Markets 47

Companies Will Expand Surveillance to Gather Data	48
Once Collected, Data Can Be Repurposed	49
Do Citizens Own Their Data?	50
Data Authorization Focuses on Consent, Not Ownership	52
Limited Data Protections Put Privacy at Risk	54

Institutionalizing Inaccuracy 56

FR is Inaccurate Among Most Populations, Including Children	57
Humans Make Final Matching Determinations	58
Systemic Discrimination Feeds Back Into Surveillance Technology	60
Maintaining Accuracy Requires Sustained Resources and Training	62
Difficulty of Assessing Accuracy in Preventing Low-Probability Events	64
Local Officials Must Determine Accuracy Among Heterogeneous Products	64
Limited Regulation of Surveillance Technologies	65
Courts Become Ultimate Arbiters of Accuracy	66
Excitement Over a Technical Fix Leads to Entrenchment	67

National and International Policy Landscape 69

Bans and Moratoria	69
Consent and Notification Policies	71
Data Security Policies	73
Policies to Tailor Use	74
Oversight, Reporting, and Standard-Setting Policies	75
FR Expansion Without Regulation	76
Regulating FR in Schools	77

National and International FR Policy Maps 79

Our Facial Recognition Future 83

Recommendations 85

National Level	86
State Level	88
School and School District Level	89

Acknowledgements 92

References 93

Further Resources	110
Appendix A: Questions for School Administrators and Teachers to Ask Facial Recognition Companies	111
Appendix B: Questions for Parents, Guardians, and Students to Ask Schools and School Districts	112
For Further Information	114



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.

Acronyms

APPI	Act on the Protection of Personal Information (Japan)
BIPA	Biometric Information Privacy Act (Illinois)
CCTV	Closed-Circuit Television
DARPA	Defense Advanced Research Projects Agency (United States)
DPA	Data Protection Authority (Sweden)
EEA	European Economic Authority
FBI	Federal Bureau of Investigation (United States)
FDA	Food and Drug Administration (United States)
FERET	Facial Recognition Technology Program (United States)
FERPA	Family Educational Rights and Privacy Act (United States)
FR	Facial Recognition
FTC	Federal Trade Commission (United States)
GDPR	General Data Protection Regulation (Europe)
K-12	Kindergarten through High School
NCES	National Center for Education Statistics (NCES)
NIH	National Institutes of Health (United States)
NIST	National Institute of Standards and Technology (United States)
SHIELD	Stop Hacks and Improve Electronic Data Security (New York)
SRO	School Resource Officer
TAP	Technology Assessment Project
TSA	Transportation Security Administration (United States)

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

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

inaccuracy. Because FR is automated, it will extend these effects to more students than any manual system could.

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.

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



Burst (CC-o)

originally instituted for school security, but in practice became most often used for monitoring student behavior. Considering

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

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

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.

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, 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, p. 79](#)). 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

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

FR must also provide multiple opportunities for review and change, as the technology’s consequences become clearer.

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 appendices to the **full report** we have also provided stakeholders (e.g., parents/guardians, students, and school administrators) with sample questions to help them evaluate the technology.

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.

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.

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**.

Introduction

KEY TAKEAWAYS

- Facial recognition (FR) algorithms process data from an individual's facial features to identify unique matches, often using both private and publicly available data including social media.
- Law enforcement has used FR since 2001.
- The global FR industry is currently valued at \$3.2 billion.
- Schools have begun to use FR as a security measure to supplement or replace other interventions such as school security officers and metal detectors.
- Using an analogical case comparison method, we identified and examined five implications: exacerbating racism, normalizing surveillance, defining the acceptable student, commodifying data, and institutionalizing inaccuracy.

Facial recognition (FR) is a technology capable of identifying or verifying one's identity based on an image of a face. Generally, FR systems work by systematically comparing the features and measurements of a person's face with facial images in a database in order to find a match. Though long considered science fiction, this technology is increasingly commonplace around the world. It is now used for identity detection and verification across sectors, including law enforcement, security, retail, employment, and education. Many consider FR to be a particularly useful identity verification measure compared to others such as passwords, PINs, or fingerprints, as someone's facial data is unique and difficult to steal or replicate.

How Does the Technology Work?

FR systems treat faces as collections of data points (Thorat et al., 2010). Though the exact methods vary from company to company and

between uses, the basic steps are as follows. The first step is face detection: a camera is directed towards a face, and then detects and recognizes it as a face. Then, the facial image is captured and analyzed, most often as a two-dimensional image. During analysis, FR technology reads a face's geometry and

makes many measurements, such as the distance between eyes, length and width of face, etc. (Thorat et al., 2010). The software also identifies key facial landmarks, and facial features are coded into a set of numbers called a faceprint. Finally, once the faceprint is numerically coded, the system will run this formula against a database of other known faceprints, seeking a match (Mann & Smith, 2017). Because FR requires a clear image in order to measure and code a face, the technology is usually rendered ineffective and non-functional when the face is obscured, such as by wearing a hat, sunglasses, or a mask, or if image quality is poor (Simonite, 2020). This limitation suggests that the technology's utility will be much lower during the COVID-19 pandemic, as most people wear masks when they venture out in public and will likely continue to do so for the foreseeable future.

Depending on what specific FR process is being used and what databases the system is connected to, this matching process may generate additional information about the face scanned, including a person's name and other personal information. This is facial identification, which is what police officers do when they scan the faces of witnesses or suspects against a database in hopes of learning their name and address. This is a one-to-many match (Thorat et al., 2010). Another FR process is authentication or verification of a user's identity, which means that the system confirms that the face scanned indeed belongs to whoever the subject said they were; for example, this is what occurs when individuals use FR to unlock their smartphones. This is a one-to-one match (Thorat et al., 2010).

Facial recognition technologies have two categories of error: False positives and false negatives.

A false positive result incorrectly indicates that an image is a match. A false negative result incorrectly indicates that an image is not a match. When the result correctly indicates whether or not the person is a match, that is a "true" positive or negative. Accuracy is often reported using sensitivity and specificity statistics, which describe the true positive and negative rate of a technology respectively. During the development phase both rates can be improved with technical advancements, but after that, sensitivity and specificity are always a trade-off, and can be adjusted to optimize one at the expense of the other depending on the way the technology is being used. In some cases, it may be so important that the correct person is not missed that it is worth falsely identifying some people, while in other situations, false identification may carry heavy penalties so it would be preferable to correctly identify when someone is not a match, even if it means some matches may go undetected. Many facial recognition companies allow users to adjust these thresholds.

Facial Recognition's History

Widely considered to be the father of FR, Woodrow Wilson Bledsoe developed a precursor in the 1960s (Gates, 2011). For years, researchers innovated on Bledsoe's approach, identifying standard facial markers for analysis (Thorat et al., 2010). FR analysis was manual until 1988 when Sirovich and Kirby developed the Eigenface approach, which uses principle component analysis to efficiently represent pictures of faces (Turk & Pentland, 1991). The Eigenface method bases face recognition on just a few features that best approximates a given set of facial images (most often, the database that the test image is being compared to), rather than basing recognition on the facial features that we would intuitively consider most important, such as eyes, noses, and ears (Turk & Pentland, 1991). This method allows systems to represent subjects with a relatively small amount of data, allowing FR to function automatically. In the years following the development of the Eigenface approach, researchers improved computing techniques so that FR could be done in real-time.

In 1993, the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST), both US government agencies, created the Facial Recognition Technology (FERET) Program (Gates, 2011). FERET played an important role in advancing FR research, establishing the viability of automatic FR systems and further developing the technology (National Institute of Standards

and Technology [NIST], 2017). It also created a database of thousands of facial images to aid in the development of FR algorithms and provide a testing set to train these algorithms (Gates, 2011). Images for this database were collected between August 1993 and July 1996 through photography sessions with 1,199 individuals, producing 14,126 images for the database (NIST, 2017). No information is available from NIST or FERET about any attempts to ensure that this database was inclusive and representative in terms of race or gender.

FR was first used for security on a large scale at the 2001 Super Bowl, when law enforcement deployed it in an attempt to detect potential threats among the crowds attending the game (Woodward, 2001). It failed. The technology generated many false positives, showing that the technology did not work well in large crowds. It also generated considerable public backlash on privacy grounds (Grossman, 2001; Anderson, 2001). Nevertheless, use of the technology for law enforcement purposes has expanded considerably. Pinellas County, Florida was one of the first to implement FR systems for law enforcement purposes in 2001 (Valentino-DeVries, 2020). By 2009, Pinellas County's system regularly provided police officers with FR cameras to photograph and cross-check suspects' faces with the Florida Department of Highway Safety and Motor Vehicles's photo database on-the-go in real time (Spaun, 2011). By 2011, in the largest biometric installation in an airport to date, Panama brought FR into its Tocumen airport for law enforcement purposes (Kumar & Bansal, 2015). FR is increasingly used in schools and on college campuses, widely in

China but also in the United States and the UK. (Sutton, 2019; Samuel, 2020; Holloway, 2019; Alba, 2020; Heilweil, 2020a; Paul, 2020).

The FR Landscape Today

Today, FR is a \$3.2 billion industry populated by both start-ups and large companies (Singh, 2019). It is projected to reach \$7 billion by 2024 (Singh, 2019). Most of the major players are based in the United States and China, and the world's "Big Five" technology companies—Alphabet (Google), Apple, Facebook, Amazon, and Microsoft—are all playing lead roles in its development and deployment. However, many FR companies are small start-ups (e.g., Megvii, CloudWalk Technology, SenseTime) rather than household names and are based in China.

FR is now used widely—with very little regulation—across the world (See [Map A, p. 79](#)). China, for example, has a vast network of cameras implemented in public spaces throughout the country. By its own estimate, it has approximately 200 million FR cameras (Feng, 2019). Public opinion research indicates that Chinese citizens embrace and accept the use of technology in daily life more than citizens of the US, UK, and Germany (Kostka et al., 2020). More than one-third of Chinese citizens use FR in their daily lives, compared to the US and the UK where over half of the populations report never using this technology (Kostka et al., 2020). FR is used in

public spaces to track movements and even flag petty crimes. People can use FR to gain entry to home and work, check in for travel, and even pay for food at restaurants (Leong, 2019). Most recently, in December 2019, China instituted new regulations requiring that anyone registering a new mobile phone must submit to facial scans (Griffiths, 2019). Presently, there are no laws in China regulating the use of FR.

FR is increasingly used in schools and on college campuses, widely in China but also in the United States and the UK.

Meanwhile in the United States, police departments and federal agencies such as Immigrations and Customs Enforcement have used Amazon's FR software, Rekognition, since 2017 (Harwell, 2019a). Law enforcement uses Rekognition to identify individuals quickly by photographing suspects' faces and running that image against a database of other images, often obtained from mugshots and driver's license photos (Harwell, 2019a). However, since an MIT Media Lab study found that Rekognition identified darker-skinned women as men 31% of the time, it has been criticized for being inaccurate and discriminatory (Singer, 2019; Buolamwini & Gebru, 2018; Raji & Buolamwini, 2019). In June 2020, Amazon responded to these claims of racial bias by banning police from using Rekognition for one year, in order to give

Congress time to pass FR regulations (Weise & Singer, 2020).

Recently, US law enforcement officials have begun to use a FR app developed by Clearview AI, a controversial American technology company (Hill, 2020a). Clearview AI's app allows users to take a photo of a person, upload it, and attempt to match it with a large database of photos harvested from the Internet. The database includes more than three billion images that have been scraped from social media websites, including Facebook, Twitter, and LinkedIn, without user consent (Hill, 2020a). This three billion image database dwarfs even the Federal Bureau of Investigation's (FBI) FR database, which has 411 million images (Hill, 2020a). This app can be used on-the-go and purports to identify faces even with low quality images. More than 600 law enforcement agencies in the United States, from local police departments to the FBI and US Department of Homeland Security, have used Clearview AI to solve crimes ranging from identity theft to murder (Heilweil, 2020c). Though law enforcement agencies have used FR since the early 2000s, the use of Clearview is significant because it means that law enforcement agencies are no longer constrained to using only government-provided images, such as driver's license photos (Hill, 2020a). This widens the net of citizens who can potentially be identified with FR.

Clearview AI has provoked even further scrutiny due to the fact that, despite the company's insistence that its technology is provided only to law enforcement and a few private companies, a recent New York Times

investigation revealed that the app is also used by investors and friends of the company (Hill, 2020b; Heilweil, 2020b). Using their personal Clearview logins, wealthy investors, bankers, retailers, and actors report being able to use the app to identify their customers, clients, or even strangers (Hill, 2020b). Because this app is equipped to allow users to identify strangers on the street and gain information on who they are, where they live, and what they do, the unregulated use of this technology raises major privacy concerns (Hill, 2020b).

FR has also become a common method for identity verification in the United States and around the world. Apple's Face ID and Microsoft's Windows Hello are likely the most popular products recognizable to consumers. Both primarily use the technology as an identity verification tool to unlock devices, rather than using a PIN or password. These companies' products, such as the iPhone, which uses the technology for device unlocking, have been extremely important in bringing FR technology into consumers' daily lives. In 2017, Apple's first phone with FR, the iPhone X, quickly sold out, suggesting that its FR system was not a barrier for users. Google's FaceNet and Facebook's DeepFace are less popular, though the companies continue to develop them. Facebook claims that DeepFace can determine whether two faces in different photographs belong to the same individual at a 97.35% accuracy rate, even when lighting is poor or if the individual looks different between the two photos. This rivals the average human's accuracy rate for the same task, which is 98% (Bohannon, 2015; Taigman et al., 2014). For years,

Facebook used it to streamline the process of tagging people in photos on the platform, although the company removed this feature after it was sued (Acquisti et al., 2014).

In June 2020, in the wake of nationwide protests against the deaths of George Floyd, Breonna Taylor, and Ahmaud Arbery and a national resurgence of conversation about anti-Black racism and police brutality, IBM, Amazon, and Microsoft all publicly committed to limiting development and sale of FR technologies until federal regulation is passed (Greene, 2020). The companies cited concerns about the technology's racially biased nature. As stated above, Amazon banned police from using Rekognition for one year (Weise & Singer, 2020). Microsoft committed to not selling its FR technology to police departments until there is a federal law regulating the technology (Greene, 2020). Finally, IBM publicly promised to stop developing FR altogether because of its contribution to racial profiling and mass surveillance (Weise & Singer, 2020). However, as noted above small start-ups are leading FR innovation, rather than these big players.

School Security and Facial Recognition

FR is slowly being integrated into schools around the world. In the United States, localities from New York to Texas to Oklahoma have begun to use the technology (Simonite & Barber, 2019). But when schools in France and Sweden attempted to use FR, they were fined and asked to remove it in 2019 because the use violated the European

Union's (EU) General Data Protection Regulation (GDPR) (Kayali, 2019).

Schools have largely deployed FR as a security measure. Traditionally, school security measures have included locking or monitoring doors and gates, school resource officers (SROs), metal detectors, closed-circuit television (CCTV) security cameras, emergency preparedness drills, and violence prevention programs. During the 2015-16 school year, 94% of public schools in the United States controlled entry by locking or monitoring doors, 81% used security cameras, and 4% used random metal detector checks (National Center for Education Statistics, 2019). Indeed, school security is a \$2 billion industry. But in recent years, schools have been searching for more accurate and unobtrusive measures, particularly given the rise of school shootings in the United States (Robinson, 2018). To many, FR seems to be a perfect solution because it offers more capacity to monitor who is on campus and what people are doing than humans combing through security footage. The idea is that FR will detect if there is someone on school grounds who is not supposed to be there (for example, someone whose face does not match any entries in a database of student and staff faces, or who may be on a "watchlist"). It could then deny those people entry to particular classrooms or the school building itself. Of course, this assumes that FR is indeed an accurate and unobtrusive measure for all demographics: throughout this paper, we will explain why this is not the case. Besides school security, FR can be used in schools to take attendance, admit students and faculty into classrooms, pay for lunches, or check out library books.

As suggested above, there are no federal, state, or local policies explicitly regulating FR in schools anywhere in the world. This lack of regulation leaves students unprotected from the negative and potentially unforeseen consequences of FR in schools. Though the United States does have the Federal Educational Rights and Privacy Act (FERPA) of 1974, which may apply to FR in schools because it defines 1) who may access student records and for what purposes, and 2) the rights of students and parents to view and correct student records, the law was written with non-digital records in mind, and, despite a 2002 update, does very little to protect student privacy in the digital age.

In October 2019, the French Data Protection Authority (CNIL) released a non-binding opinion that the plan of two French high schools to use FR technology to control entry violated the EU's GDPR, because less intrusive methods of achieving the same ends were available (Kayali, 2019). Earlier that year, Sweden's Data Protection Authority (DPA) found that it was not possible for students to provide sufficient consent to a school FR program, due to the power imbalance between the students and the school (BBC News, 2019b). The DPA issued the country's first fine for GDPR violations. Despite these rulings, the GDPR does not explicitly regulate FR, in schools or elsewhere, beyond placing FR data into the broader category of sensitive personal data that requires additional protection. Evidently, there is

There are no federal, state, or local policies explicitly regulating FR in schools anywhere in the world. This lack of regulation leaves students unprotected from the negative and potentially unforeseen consequences of FR in schools.

an international lack of policy and legal clarity on the issue of FR in schools. The analysis contained in this report is designed to identify the technology's most serious implications, in the hope that it can shape policy discussion.

Analogical Case Comparison: Our Analytic Approach

We adopt an analogical case comparison approach to understand the implications of deploying FR in schools. By analogical case comparison, we mean systematically analyzing the development, implementation, and regulation of previous technologies in order to anticipate how a new one might emerge and the challenges it will pose.

Policymakers often argue that they cannot adequately regulate science and technology in the public interest because innovation moves so quickly and its consequences are unpredictable. But humanists and social

scientists who study emerging science and technology, from science and technology studies (STS) scholars to bioethicists, teach us that innovations are more predictable than we think, and therefore many of their moral, social, economic, environmental, and public health challenges can be anticipated early and addressed in the development process and/or through public policy (Stilgoe et al., 2013).

Innovations are more predictable than we think, and therefore many of their moral, social, economic, environmental, and public health challenges can be anticipated early and addressed in the development process and/or through public policy.

These scholars offer two important lessons for analyzing the consequences of emerging technologies. First, science and technology tend to reflect the social and political contexts in which they are developed. In the privatized and competitive health care market in the United States, for example, biomedical innovation tends to emphasize technical novelty and sophistication rather than, and sometimes to the exclusion of, diagnostic or therapeutic utility (Parthasarathy, 2007). Second, controversies over previous technologies offer insights into the kinds of concerns and resistance that might arise, groups who might be affected, and solutions that might be feasible with emerging innovation. For example, limiting

government surveillance and maintaining individual privacy has long been a priority for citizens, especially in the Western world. This has led scholars and interest groups to demand extra protection of biological samples collected for scientific purposes, because they fear they might be accessible to law enforcement officials (Krimsky & Simoncelli, 2010). They have also challenged the collection of social media passwords from travel visa applicants, citing potential constraints on freedoms of speech (Cope et al., 2017).

Building on these insights, the University of Michigan's Technology Assessment Project (TAP) has developed a process to use analogical case comparison to enhance our understanding and governance of emerging science and technology, which

we use in this report. Guston and Sarewitz (2002) argue: "Studying past examples of transformational innovations can help to develop analogies and frameworks for understanding and anticipating societal response to new innovations." This analogical case comparison approach joins a suite of methods designed to anticipate the consequences of emerging science and technology in order to better govern them. This includes scenario-planning and other stakeholder engagement exercises (Kuzma et al., 2016; Selin, 2011), initiatives to help scientists and engineers reflect on the ethical, social, and environmental consequences of their choices as they work in the laboratory (Fisher et al., 2006), and deliberative

democratic efforts that value lay insights about the world and community experiences with technology (Hamlett et al., 2013; Stirling, 2008).

To study FR in schools using an analogical case comparison approach, our research team began by identifying two types of analogs. The first were technologies that seemed similar to FR in their basic functions, such as CCTV and predictive policing. The second were technologies that seemed to have similar moral and social implications as FR, such as databases that collect genetic, medical, and lifestyle information (known as biobanks) that raise concerns about consent and ownership of biometric data. It is important to note here that we define analogical technologies broadly, to include interventions that have technical, human, and physical components (what scholars refer to as “sociotechnical systems” (Bijker, Hughes, and Pinch, 1987; Mackenzie and Wajcman, 1985). Both school-based law enforcement (known as school resource officers) and metal detectors, for example, function as important

surveillance technologies for the purpose of our study.

We first investigated both types of technologies, reading scholarly literature and doing some research into primary sources to fully understand their development, implementation, consequences, regulation, and associated controversy. This helped us begin to anticipate the consequences of using FR technology in schools. This process also led us to identify other previous technologies that might provide additional insights, such as the breathalyzer that checks for blood alcohol content but has raised multiple concerns about accuracy.

In the second phase of research, we fully analyzed the histories of these interventions. We also followed up on potential implications that we had not considered during the first phase such as how law enforcement and metal detectors in schools, while designed to maintain safety, often exacerbated racism. We continued this identification and analysis of previous technologies and their implications

To study FR in schools using an analogical case comparison approach, our research team began by identifying two types of analogs. The first were technologies that seemed similar to FR in their basic functions, such as CCTV and predictive policing. The second were technologies that seemed to have similar moral and social implications as FR, such as databases that collect genetic, medical, and lifestyle information (known as biobanks) that raise concerns about consent and ownership of biometric data.

in an iterative fashion. We then analyzed our analogical case studies together and used them to identify five main implications of using FR in schools. What follows is based

on this research process. The list below summarizes the analogical case studies we developed and explains why they parallel FR in schools:

Analogical Case Studies

Aadhar

India's nationwide biometric system and the world's largest biometric ID system, collects multiple measurements including fingerprints, iris scans, and facial scans from citizens and assigns each a unique 12-digit ID number. Enrollment in Aadhaar is required to access welfare services, financial services, to make purchases, and to enter government buildings. It resembles FR because it gatekeeps services based on the ability to supply biometric data and widens the scope of surveillance.

Airport Security

This includes bag searches, body scanning machines, and interaction with airport security agents. All are designed to be neutral crime control strategies that are meant to ensure safety and security at the airport. However, in practice, these strategies appear to be susceptible to administrator bias and produce discriminatory outcomes.

Biobanks

Institutions that collect biological samples that are used in research. These institutions collect sensitive personal data in the name of innovation, but have been criticized for questionable privacy and security safeguards.

Breathalyzers

Devices that determine an individual's blood alcohol content by measuring the amount of alcohol in one's breath. This device requires significant resources and user training in order to maintain high accuracy levels, but is often used without maintenance or regulation and therefore fails to meet those standards, hence producing unreliable results that can have a material impact on people's lives.

Closed Circuit TV in Schools

A television system in which video signals are sent from multiple cameras to a set of monitors. CCTV has been implemented in many schools especially in the UK. This technology is similar to FR in form and function: a network of cameras surveilling students in order to increase security. These often have the effect of normalizing surveillance and widening the scope of punishable student behaviors.

Fingerprinting

The practice of collecting impressions of one's fingertips to produce unique biometric markers. Fingerprinting is used in law enforcement and as an identification tool. However, interpretations of fingerprint matches can vary from analyst to analyst. At times, it is used in schools for both security and efficiency reasons, much like FR, with the result of normalizing surveillance and making students feel criminalized.

Metal Detectors in Schools

A security technology that can alert administrators of any metal items in a student's bag, aiming to reduce the number of weapons brought into schools and therefore minimize crime and violence. Despite their stated aim to increase safety at school, they often actually made students feel less safe.

Moore vs. Regents of the University of California

A landmark 1990 Supreme Court of California decision that dealt with the issue of property rights over one's cells collected by doctors and researchers. In ruling that a patient does not have personal property rights over their discarded tissue samples, this case determined that consent and notification about data collection can be overlooked in the name of innovation.

Predictive Policing

Algorithms that aim to predict areas where crime will occur using historical data, in order to direct police to patrol locations before any specific crime has occurred. In practice, the data used reflects systematic racism and can produce inaccurate results, and the disproportionate deployment in predominantly Black and brown neighborhoods produces racist outcomes.

School Resource Officers (SROs)

Law enforcement officers placed in schools to reduce crime and control student behavior, who often target vulnerable students and produce negative psychological and social impacts.

Stop and Frisk

A crime control strategy that gave police more power to stop and question those deemed "suspicious". This was a net-widening strategy: it was often used to stop citizens who wouldn't otherwise have interacted with law enforcement. Though this strategy was purportedly neutral, it often reflected officer biases and produced discriminatory outcomes.

Overview of the Implications

Much of the public and policy discussion regarding FR technology, including its use in schools specifically, has focused on concerns about accuracy, privacy, and data misuse (Burton, 2019; Hill, 2020a). Our analogical case study approach allows us to provide a deep analysis into how these implications might take shape, while also identifying additional potential implications based on historical evidence. In this report, we focus on the following:

Exacerbating Racism

The use of FR in schools is likely to amplify, institutionalize, and weaponize existing racial biases, resulting in disproportionate surveillance and humiliation of Black and brown students. As indicated by the historical cases of stop and frisk, airport security, SROs, and metal detectors in schools, FR is poised to disproportionately target students of color and inflict upon them adverse psychological and social impacts.

Normalizing Surveillance

The analogical historical cases of CCTV and various biometric identification methods, including fingerprinting in schools and India's Aadhaar system, suggest that FR in schools will normalize the experience of being constantly surveilled. These historical cases also provide compelling evidence that FR in schools will undergo mission

creep, furthering the reach of surveillance, as administrators face temptations to use the technology for unofficial uses. Finally, we conclude that the normalization of surveillance will make students feel powerless and put their privacy at risk due to limited data protections.

Defining the Acceptable Student

FR will widen the scope of what students can be punished for, because students will be rendered far more visible to administrators. This will lead to young people being disciplined in unexpected ways. Just as the analogical cases of CCTV, predictive policing, and India's Aadhaar system discriminated among subjects by excluding or punishing certain individuals based on non-criminal characteristics outside of their control, FR in schools will privilege some students and exclude or punish others based on their adherence to social norms.

Commodifying Data

The cases of predictive policing, biobanks, and court cases over data ownership, such as *Moore v. Regents of the University of California*, suggest that the institution of FR in schools will generate new data on students, resulting in the creation of new commodities and data markets. This raises concerns about ownership, consent, and market exploitation, and may result in threats to individuals' data security and privacy.

Institutionalizing Inaccuracy

Analogical case studies of predictive policing, CCTV, fingerprinting, and the breathalyzer, which are similar to FR in their surveillance functions, teach us that establishing and maintaining accuracy is difficult and sometimes even impossible. This is because, though these technologies are marketed as objective and insulated, they are in fact influenced by human judgment, norms, and institutions.

Exacerbating Racism

KEY TAKEAWAYS

- School security measures disproportionately target and discriminate against people of color, particularly Black, Latinx, and Indigenous communities.
- FR is likely to be used disproportionately in majority-minority schools, without any meaningful resulting reductions in violence.
- FR is likely to make students feel less safe and cared for by their school.
- FR is likely to amplify, institutionalize, and weaponize existing racial biases, resulting in disproportionate surveillance and humiliation of Black and brown students and adverse psychological and social impacts.

Given the legacies of racism and colonialism across the world and cases of previous surveillance technologies, we expect facial recognition to exacerbate racism. Browne (2015) traces the racist dimensions of surveillance technologies to the early days of slavery; owners used brands, for example, to commodify and track slaves, making them feel hypervisible and powerless. Brands were, essentially, one of the first forms of biometric identification. More recently, cases of stop and frisk, airport security, school resource officers (SROs), and metal detectors indicate that FR is likely to continue to amplify, institutionalize, and weaponize existing biases, resulting in disproportionate surveillance and humiliation of Black and brown students and adverse psychological and social impacts. Because these cases are

analogous to FR in schools due to their use for security purposes and their susceptibility to administrator bias, we expect that FR will produce similar effects. That is, we expect FR in schools to target and harm vulnerable students: for example, FR is likely to increase the frequency with which Black and brown students are singled out and disciplined by school administrators. Also, because FR has higher error rates for Black and brown subjects, it is likely to malfunction for students of color more often than their white counterparts. This could have the effect of further excluding and victimizing already marginalized students.

Facial Recognition Accuracy Varies by Race

FR is less accurate in identifying people of color than white people (Harwell, 2019b; Buolamwini & Gebru, 2018). A comprehensive December 2019 National Institute of Standards and Technology (NIST) study, which examined most leading FR systems including 189 algorithms from 99 companies and developers, concluded that FR systems have “demographic differentials” that varies accuracy by a person’s gender, age, and race (NIST, 2019). These algorithms consistently showed high error rates when used on African-Americans, Asians, Native Americans, and Pacific Islanders. In fact, “Asian and African American people were up to 100 times more likely to be misidentified than white men” (Harwell, 2019b). White men are the demographic with the highest accuracy rate, with an error rate of up to only 0.8% (Harwell, 2019b; Buolamwini & Gebru, 2018). A 2018 study showed the same results: Buolamwini & Gebru’s evaluation of three different FR algorithms found that datasets are overwhelmingly composed of lighter-skinned subjects, and as a result algorithms perform best for lighter-skinned individuals, particularly men, and perform worst for darker-skinned subjects and women (Buolamwini & Gebru, 2018). The higher error rates of FR for non-white subjects mean that the technology will malfunction for them

more than it will for their white counterparts. This means that Black and brown students will be misidentified more often, or not identified at all. The consequences of this will range from inconvenient, such as barring students of color from checking out library books, to extremely damaging, such as criminal investigations. In part because of this, we strongly urge against the use of facial recognition in schools.

Black and brown students will be misidentified more often or not identified at all. The consequences of this will range from inconvenient to extremely damaging.

Disproportionately Targeting People of Color

Young people of color, particularly in the United States, have long experienced greater amounts of surveillance than their white counterparts due to a history of racist policies and practices. These policies and practices assume that these young people are appropriate targets for surveillance because they are likely to misbehave or engage in criminal acts, but these very assumptions become self-fulfilling prophecies.

SROs, police officers who have been deployed in schools, illustrate this disproportionate surveillance. They generally report to municipal police or county sheriff's offices, or in the case of some large urban districts such as Los Angeles there may be a separate police department for the school system (Brown, 2006). SROs first appeared in the 1940s,

Racist policies and practices assume Black and brown young people are appropriate targets for surveillance because they are likely to misbehave or engage in criminal acts, but these very assumptions become self-fulfilling prophecies.

just as US schools began to integrate; early adopters were either schools and districts that served large numbers of Black and Latinx students, or where Black and Latinx students were entering predominantly white schools for the first time (American Civil Liberties Union [ACLU], 2017). Some early programs, such as the "Officer Friendly" program in Chicago, were characterized as a way to "improve community relations between the city's youth and the local police department" (Mbekeani-Wiley, 2017). However, the community relations aspects of school policing quickly gave way to an emphasis on law and order.

The implementation of SROs coincided with burgeoning civil rights movements

among Black and brown youth in the 1960s. Black students in the South fought against segregation and racial violence, while Chicana students in California staged huge walkouts demanding access to college preparatory classes and culturally relevant curricula (Advancement Project, 2018; Garcia & Castro, 2011). Placing police in schools became a way for cities, states, and the federal government to coordinate against student protesters. At the same time, the growth of SRO programs precipitated policy changes that criminalized behavior that would previously have warranted a trip to the principal's office. For example, the state of Maryland made it a crime to disturb school activities soon after placing SROs in Baltimore schools (Craven, 2016). Today, over

20 states have school disturbance laws (Ripley, 2016). Always, the stated purpose is to make schools safer for children, but the result appears to be the criminalization of students by increasing the frequency of their interactions with law enforcement.

The War on Drugs in the 1980s and 1990s accelerated the practice of policing children in the name of safety. In 1985, the Supreme Court ruled that school officials, including school police, could search a student or a student's possessions without a search warrant (*New Jersey v. T.L.O.*, 1985). This is the case if the officials have a reasonable suspicion that a student has violated not just a law, but a school policy. School officials or SROs may search students if they suspect they

have an item such as a cell phone or a bottle of over-the-counter medicine, which are legal to possess outside of school (Brown, 2006). Federal law further increased police presence in schools when the Violent Crime Control and Law Enforcement Act of 1994 funded the creation and expansion of SRO programs.

Today, while most American schools do not have SROs, SROs have an outsized presence in schools that serve students of color. 51% of high schools with majority Black or Latinx enrollment have SROs on campus, in comparison to 42% in high schools overall. Black students were more than twice as likely as their white classmates to be detained or arrested at school (ACLU, 2017). Disabled students of color are at even greater risk: they are more likely to be referred to law enforcement than their white disabled or non-disabled counterparts (Alabama Appleseed, 2019). The presence of police in schools, coupled with zero-tolerance policies popular in the 1990s that expelled students after a single rule violation, have been major contributors to the school-to-prison pipeline, criminalizing predominantly Black and brown students for childhood mistakes (Nelson & Lind, 2015).

Stop and frisk is another important analogical case. This purported crime control strategy that allowed police officers to stop and question virtually anyone they wanted to, is an example of how administrator biases can render a seemingly neutral crime control strategy discriminatory. We expect that the same phenomenon will occur with FR in schools. *Terry v. Ohio*, a 1968 Supreme Court case in the United States, legitimized the practice of stop and frisk. Police officers could

stop and search citizens proactively, without probable cause for arrest, as long as there was “reasonable suspicion” that a crime had been committed (Katz, 2004; Cornell Law School, 2019). The practice was then used in many major US cities, including Chicago, Los Angeles, and Philadelphia (James, 2015). Most famously, when it was used in New York City from the 1980s until 2013, Black and brown residents were stopped at a far higher rate than their white counterparts both compared to their overall population size and the rates of crime they committed (Gelman et al., 2007). Simply being Black or Latinx seemed to provide officers with “reasonable suspicion” to stop someone. In the late 1990s, at the height of this practice in NYC, then-Attorney General Eliot Spitzer published one of the first major reports on racial disparities in stop and frisk, highlighting that Blacks and Latinxs comprised only 49.3% of NYC’s population and yet made up 83.6% of stops (Spitzer, 1999). Meanwhile, white New



NYPD, CC BY 4.0

Yorkers, who accounted for 43.4% of New York’s population, comprised only 12.9% of stops (Spitzer, 1999). Though minorities

were stopped more often than whites, they were arrested at lower rates from these stops than their white counterparts, suggesting that lower standards were used for stopping minorities, and the frequency of these stops was not related to actual crime (Gelman et al., 2007).

Finally, airport security practices are another analogy to FR in schools. Airports are spaces of heavy surveillance where the same acts and appearances may be coded differently (suspicious or non-suspicious) based on who performs them (Browne, 2015). Officers from the Transportation Security Administration (TSA) and Customs and Border Protection (CBP) in the United States are subject to only vague guidelines that allow them to search almost anyone under virtually any circumstances; it is therefore not surprising that they routinely profile by race and gender. Survey data indicates that non-white travelers are more likely than their white counterparts to be selected for additional screening and to have to undergo a greater number of additional search procedures when selected, such as pat-downs (Lum et al., 2015). Additionally, travelers of color reported having greater embarrassment during screening procedures than their white counterparts, suggesting that this process systemically humiliates and threatens people of color (Lum et al., 2015). Black women are less likely to be found with contraband than white women, and yet they are the demographic most likely to be strip searched by airport security (Browne, 2015).

School resource officers, stop and frisk, and airport security all demonstrate how law

enforcement practices that systematically surveil the population and discipline those who pose a perceived threat are consistently wielded against Black and brown people. Because these practices allow the racial biases of those who perform them to be legitimized, institutionalized, and weaponized, they have the effect of not only criminalizing and targeting minorities, but making these outcomes appear rightful.

Just as the administrators of SROs, stop and frisk, and airport security claim that these practices are neutral and only target those who pose security risks, school administrators will also likely claim that FR will not target students of color. However, just as those analogical cases legitimize the racial biases of administrators and have the effect of singling out minorities, so will FR in schools. Administrators of school FR systems will be able to claim that racist outcomes are rightful because they were produced by an algorithm, even though these outcomes are actually a result of user biases and the algorithm's lower accuracy rates for Black and brown faces. We can expect that, through these mechanisms, FR in schools will result in more Black and brown students being flagged for misbehaving or truancy, and therefore being disciplined disproportionately more than their white counterparts. Another potential outcome is that, because FR has higher error rates for non-white faces, school FR systems will fail to detect students of color: this would result in that student being flagged as an intruder and potentially being subjected to confrontation with administrators or the police and unjust punishment. In sum, because FR is poised to mimic analogous security practices by

surveilling and disciplining students in the name of school security, it is also likely to mirror the effects of these practices by unfairly targeting and punishing Black and brown students.

Adverse Psychological and Social Impacts

Some argue that FR is a neutral technology (Introna & Wood, 2002). This implies that the technology is fair and will only be used to target and punish those who are guilty. Unfortunately, this does not bear out in practice. In the cases of SROs, stop-and-frisk, and airport security, there is evidence that people of color are penalized for behaviors that are seen as normal among white people (Henning, 2013). These practices also contribute to a culture of fear. New York residents who have been subject to stop and frisk, for example, report “lasting emotional, psychological, social, and economic harm” as a result of these stops, which may entail inappropriate touching, sexual harassment, police brutality, humiliation, and violence, all in public and at the hands of police officers (Center for Constitutional Rights, 2012). Other studies similarly report that living in neighborhoods with aggressive policing tactics can negatively affect one’s mental health, producing feelings

of non-specific psychological distress and increasing the likelihood of post-traumatic stress disorder (Sewell et al., 2016; Ross, 2016). Further, there is evidence that stop-and-frisk tactics can have negative effects on physical health as well, increasing the likelihood of diabetes and high blood pressure (Ross, 2016). As a result of this conduct, entire communities of color in New York have lived in fear of police and expect that abuse by law enforcement is a normal part of daily life (Center for Constitutional Rights, 2012).

Many New York residents report that pervasive fear of police has impacted their daily routines, by spurring them to change their hairstyles and clothing to minimize attention, change their routes to avoid walking in public or nearby police, and constantly carry identification and other important documents.

Many New York residents even report that this pervasive fear of police has impacted their daily routines, by spurring them to change their hairstyles and clothing to minimize attention, change their routes to avoid walking in public or nearby police, and constantly carry identification and other important documents (Center for

Constitutional Rights, 2012). In this way, stop and frisk—a seemingly neutral crime control strategy—became a vehicle to amplify existing racial biases in a violent manner that increased surveillance, humiliation, and distrust of authority among Black and brown New Yorkers, and ultimately exerted control over marginalized New Yorkers’ day-to-day lives.



Wiki user PQ77wd, CC BY-SA 4.0

We see similar impacts from the use of metal detectors in schools. First implemented in the 1990s, they were intended to reduce or eliminate the presence of weapons such as guns and knives on school grounds, thereby preventing violence. Although it would curtail students’ Fourth Amendment rights against search and seizure, leaders hoped it would keep schools safe (Ferraraccio, 1999). Use of metal detectors rose further after the 1999 Columbine school shootings (Jonson, 2017). But as with SROs, metal detectors are more prevalent in schools where the majority of students are Black or Latinx. They are used disproportionately in schools located in urban

or high crime areas (Hankin et al., 2011). One study analyzing data from the National Center for Education Statistics (NCES) 2007–2008 School Survey on Crime and Safety, found that 91% of public schools that perform daily metal detector searches of students are high-violence, majority-minority schools. Importantly, among all high-violence schools, those with majority-minority enrollments are significantly more likely than majority white schools to use metal detectors on their students (Gastic & Johnson, 2015).

Metal detectors seem to have an overall negative effect on students. Despite extensive research into their effectiveness in reducing school violence, there are no conclusive findings that these technologies have a significant effect on school safety (Hankin et al., 2011). At the same time, a growing body of research has found that they significantly alter students’ school experience. Metal detectors decrease students’ sense of safety, even after controlling for the level of violence at the school (Gastic, 2011; Hankin et al., 2011), while their feelings of being cared for by their school and trusting their administration decline (Jonson, 2017). And, a large, multi-site survey of middle school students found that those who perceive their schools to be more unsafe were more likely to be both the victims and the perpetrators of relational aggression, which is harm caused by damaging someone’s relationships or social status (Elsaesser et al., 2013). The case of metal detectors in schools shows that instituting strict law enforcement measures in the name of school security can often have the opposite effect than what was intended: rather than making students feel safer at school, students feel criminalized, as if their

schools distrusts them, and more anxious and unsafe.

Conclusion

In sum, we have a long history of surveillance practices and policies that appear, on their face, to be objective and focused on public safety. But in practice, they reflect the racial biases in law enforcement and the broader society and reinforce the incorrect assumption that people of color are, by their very existence, prone to criminality and appropriate targets for increased surveillance. We might assume that FR is likely to be less obtrusive and more accurate. But like previous interventions, this technology is part of racially-biased social systems. Where and how it is deployed will be determined by humans (school administrators and city officials), matches will be certified by humans (law enforcement officers), and so too will definitions of misbehavior and criminality. Hence, just as human biases were funnelled into the use of SROs, stop and frisk, airport security, and metal detectors, thus legitimizing racist outcomes, so will FR systems in schools.

It is likely that FR's lower accuracy for Black and brown faces, as well as the racial biases of human administrators of the system, will result in Black and brown students being disproportionately flagged by the system for disciplinary reasons. Another possible outcome is that the technology will malfunction more often for Black and brown students, which could result in them not being able to pay for lunch, check out library books, enter campus, or be marked "present" for class. The high error rate of FR for students of color could also result in them being flagged as an intruder if the system fails to recognize them as a student. This would result in Black and brown students feeling further criminalized and alienated on campus, which would certainly diminish their ability to receive a quality education. It is difficult to imagine how this technology could be deployed without burdening children of color disproportionately, in a way that is likely to have enormous psychological and social effects. Therefore, we urge against the implementation of FR in schools.

Normalizing Surveillance

KEY TAKEAWAYS

- FR systems will make surveillance a part of everyday life for young people.
- Surveillance installed for one purpose will be expanded to other uses, without explicit consent.
- Because FR systems are developed using multiple sources of data, they will likely be used to track student activities far beyond school grounds.
- Students are resentful of being surveilled at school because they experience loss of privacy and freedom.
- Students feel criminalized and powerless when faced with school surveillance systems.

Like FR, CCTV and older forms of biometric identification were designed and implemented to increase public safety in an efficient manner. But, as we demonstrate below, they have been more effective in making surveillance part of our everyday lives and eroding our privacy. We found that implementation of past surveillance technologies produced mission creep and feelings of powerlessness among students, and that limited data protections put privacy at risk. Given this history, we expect that FR will normalize and entrench the experience of being constantly surveilled. We expect that this will result in feelings of powerlessness and lack of autonomy among students, similar to what occurred in schools with CCTV systems. This can be quite damaging

psychologically and emotionally. Because we anticipate that FR in schools will normalize surveillance, erode privacy, and inflict damaging psychological effects on students, we strongly advise against it.

Technology Expanding the Reach of Surveillance

The United Kingdom has widely used CCTV in schools for suspect identification and crime deterrence. But, studies show that CCTV does not make students feel any safer or meaningfully reduce crime (Taylor, 2013). Because these cameras are not constantly monitored, their presence does not actually prevent crime or mitigate its effects—no

one would be alerted of a crime or be able to intervene until it was too late. In addition, the cameras have been shown to often simply displace crime to locations out of view, rather than actually reducing the number of crimes committed (Taylor, 2013).

Not only does CCTV often fail to achieve its intended purpose, but it has also been deployed for unofficial uses: that is, monitoring student behavior and enforcing compliance. Faced with the temptation to use this technology to monitor student behavior, administrators often do so even though this is not the stated purpose of the technology. As a result, use of CCTV in schools casts a wider net on which students may be disciplined and for what offenses. For example, CCTV is used to identify truancy, bullying, and smoking, among other aberrant behaviors on

Not only does CCTV often fail to achieve its intended purpose, but it also gets deployed for unofficial uses: that is, monitoring student behavior and enforcing compliance.

campus, and discipline students accordingly (Taylor, 2013). While this increased surveillance could provide early warnings for students who struggle with behavioral or other problems, it also, as we discuss in the next section, implicitly enforces a narrow range of acceptable behavior among young

people and suppresses their individuality. And the implementation of CCTV in schools contributes to a normalization of pervasive surveillance in society, habituating young people to constantly being observed (Taylor, 2010). Interviews with students whose schools had CCTV systems revealed that they highly valued their privacy and often took action to resist surveillance. Students reported only being comfortable with this privacy infringement in cases in which there was a strong justification, such as for school security, rather than for monitoring student behavior (Birnhack et al., 2017).

Similarly, during the 1980s—a period of heightened concern about child kidnapping—many schools began to fingerprint their students in the hope that it could help locate missing children and serve as a deterrent to potential kidnappers who would now know that children everywhere were being fingerprinted (Bridgman, 1983). This practice was soon normalized, and in recent years fingerprints have become a tool for identity verification and payment in schools. This is widespread in the UK, where more than a million secondary school students have been fingerprinted (Kobie, 2016).

Finger scanners are used to pay for lunch, take attendance, enter and exit buildings and rooms, and access lockers, computers, printers, and books. Supporters say that it expedites long lines, prevents theft, removes stigma for students who have free or reduced lunch, and is a more secure method

of verifying identity (Gray, 2007). But, by making surveillance a primary part of their environment, this practice tells children that it is normal and unremarkable to give



U.S. Air Force photo by Airman 1st Class Randahl J. Jensen

away biometric data and have it used to track their locations, purchases, and activities. Some also worry that it criminalizes children by applying a system in schools that is traditionally used in the criminal justice system (Brennan, 2017). Because FR, like fingerprinting, is also a biometric technology that would be used for security and efficiency purposes, it is reasonable to conclude that FR in schools would similarly normalize surveillance, criminalize students, and create a culture of permissiveness about personal data.

Aadhaar, India's biometric surveillance program and the largest biometric ID system in the world, has also expanded and normalized surveillance in ways that may be predictive of the potential consequences

of FR (Perrigo, 2018). In India, citizens' access to most public and private services, including welfare, pensions, mobile phones, financial transactions, and school and work enrollment, is determined by whether they have enrolled in the nationwide Aadhaar system (Goel, 2018). If citizens are not enrolled in Aadhaar, they are blocked from accessing these services. This means that it is now nearly impossible for Indians to do many normal activities without providing their Aadhaar ID, which is tied to their sensitive biometric information (Perrigo, 2018). In order to enroll in the system, citizens must provide their personal biometric data including fingerprints, iris, and facial scans. To date, 1.2 billion Indians (99% of India's adult population) have been enrolled in Aadhaar (Perrigo, 2018). After someone enrolls in the system, their data is continuously added to a centralized database as Aadhaar users access services (Arudpragasam, 2018). This means that, in addition to controlling access, Aadhaar can be used to track everything one does and everywhere one goes each day. Under Aadhaar, the government can constantly surveil everyone. People have no guarantee that anything they do is private (Jain, 2019).

There is also concern that this type of state surveillance creates the opportunity for personal information to be weaponized, particularly in the absence of any data protection laws (though such a law may exist soon: India's Supreme Court ruled in 2017 that privacy is a fundamental right for all citizens, and the Personal Data Protection Bill of 2019 is currently tabled in the Indian Parliament) (Kodali, 2019; McCarthy, 2017; Personal Data Protection Bill, 2019). For

example, the sale of health data can be used against individuals if insurance companies charge them higher premiums for pre-existing conditions (Kodali, 2019). Because FR is also a biometric system that is equipped to control student access to resources, track their movements and activities, and collect sensitive data just like Aadhaar, it is likely that FR will also have the result of normalizing surveillance and eroding student privacy.

Students Feel Powerless

Studies also suggest that these surveillance technologies had negative psychological impacts on students. In interviews, students expressed their need for privacy at school, specifically their wish to be able to express certain emotions in public without being surveilled (Taylor, 2010).

Students reported being highly resentful of CCTV systems: they stated that the technology undermined their privacy and represented the school's criminalization and distrust of them (Taylor, 2013). Interviews also revealed that many children who attend schools with CCTV cameras are not clearly informed by administrators about how the cameras work, leading students to be unsure of when they were and were not being surveilled (Birnhack et al., 2017). Finally, students also reported a sense of resignation and internalization of authority: though many resented the loss of privacy that CCTV represented, they felt they had no power to

change this system and had to simply accept that their behavior would be observed and controlled (Taylor, 2013).

In the 1980s, when schools were fingerprinting children out of concern that they would be kidnapped, there was concern that this fingerprinting could have similar impacts as CCTV in schools has today. Parents were concerned that this practice would needlessly involve children in criminal investigations and “create an atmosphere of unfounded fear”, even though the odds of them actually being kidnapped were miniscule (Bridgman, 1983). One can easily imagine that a schoolwide FR system will produce similar effects, since they have the same widespread video surveillance capabilities as CCTV (with the additional

Parents were concerned that fingerprinting would needlessly involve children in criminal investigations and “create an atmosphere of unfounded fear”, even though the odds of them actually being kidnapped were miniscule.

ability to biometrically identify students in real-time) and would collect biometric information for security purposes just like fingerprinting.

Conclusion

FR is poised to expand surveillance beyond even the scope of CCTV, fingerprinting, and Aadhaar, because it will collect biometric data and be able to track all student actions throughout the school day: arrival and departure times, where the student goes and when, library books checked out, and even what the student eats. As it combines more data, we expect that FR will significantly normalize and entrench surveillance among one of our most vulnerable populations: young people.

Further, these analogical cases indicate that expanded surveillance inflicted feelings of powerlessness, resentment, fear, mistrust, and criminalization. Since FR in schools will expand surveillance even further than these cases, we expect that the negative psychological effects will be more pronounced. We expect that such surveillance of our children will teach them that it is normal to have little autonomy over their

personal data. In an environment in which students have no control over their biometric data, they are likely to leave school with a sense of powerlessness and a distorted understanding of whether and how they can and should protect their data privacy. Teaching students that they are distrusted, criminalized, and powerless in school, a place where they should feel safe, will likely have harmful impacts on their education and development. Finally, any hacks or breaches of this data will have long-lasting effects, following students throughout their lives—unlike with most digital security, where breaches can be remedied by updating a password, facial data breaches are much more harmful. One can change their password, but they will never have any other face. In sum, it is unlikely that the benefits of FR in schools will outweigh the risks of normalizing surveillance, eroding privacy, threatening data security, and inflicting numerous harmful psychological effects on students, we strongly oppose the implementation of FR in schools.

Defining the Acceptable Student

KEY TAKEAWAYS

- FR is likely to expand definitions of deviant and criminal behavior, and punish students who don't fit within narrow standards of acceptability.
- Surveillance systems tend to treat the characteristics and behaviors of white, cisgender, straight, and non-disabled students as the norm, further marginalizing others.
- Students may try to avoid FR surveillance and law enforcement by forgoing medical attention and other critical services.
- Students who deviate from dominant social norms may be excluded from basic services like paying for lunch, accessing facilities, easily checking in for class, and having their parents participate in school activities.

The histories of CCTV, predictive policing, and biometric surveillance suggest that FR will discipline the identities and behaviors of young people in unexpected ways. We might expect that the technology might have a deterrent effect, reducing misbehavior. But, these analogical cases suggest that FR will target students whose behaviors, identities, and appearances do not constitute misbehavior, but simply fall outside dominant social norms. Outcomes of analogical cases have shown that benign expressions of individuality are likely to be reclassified as problematic or threatening, resulting in subjects feeling forced to alter their behaviors. Analogical cases also indicate

that this mechanism will result in further marginalization of already vulnerable groups. These analogies predict that the implementation of FR in schools will result in certain students being disciplined or flagged more frequently, or having the technology malfunction on them more often, for non-criminal reasons such as (but not limited to) ways they express themselves including clothing and hairstyles, their race and ethnicity, their socioeconomic status, and their disability status. In this way, the implementation of FR in schools will have the result of defining a specific “acceptable” student and punishing those who do not fit that mold. Because FR in schools is poised

to criminalize innocent expressions of individuality, we strongly advise against it.

Reclassifying Expressions of Individuality

UK schools use CCTV widely as a purported safety measure; approximately 85% of UK secondary schools have these systems (Taylor, 2011). The technology has become an important tool to monitor and discipline student behavior, and those who monitor the footage take some latitude in enforcing the rules (Taylor, 2013). Students reported that the biases of those who monitor the CCTV feeds appeared to influence their decisions to discipline a student for misbehavior. They reported that “...discrimination was purely the result of the camera operators’ propensity to derive suspicion from stereotypical interpretations of an offenders’ appearance and behavior” (Taylor, 2013). Students reported that their style of dress was a signal that often determined whether they were disciplined or not: “...certain styles of dress had become shorthand for deviancy, particularly how young people wearing hoodies were susceptible to being labelled as deviant or criminal” (Taylor, 2013). Because the human biases and assumptions of those who processed the footage played an important role in the administration of CCTV, non-criminal expressions of individuality were reclassified as problematic. This meant that the technology resulted in the creation of a narrow definition of an “acceptable” student—that is, students who were dressed in ways deemed respectable—and resulted

in the exclusion and punishment of students who didn’t fit that definition. Because FR in schools will similarly surveil students, we would expect to see the same outcome.

Further Marginalizing Vulnerable Groups

Minorities, women, disabled, and gender non-confirming people are made hyper-visible to identification and surveillance methods and ultimately, further marginalized. This is because the characteristics and behaviors of these groups may fall outside those set by individuals usually defined as the norm: white, cisgender, straight, and non-disabled. For example, SROs are 2 to 4 times more likely to refer students with disabilities to law enforcement than their non-disabled peers, an effect that was compounded for disabled students of color (Alabama Appleseed, 2019). Black boys with disabilities were more likely than any other group of students to be arrested or referred to law enforcement. Further, FR will marginalize these students because it is simply less accurate at identifying them: minorities, women, disabled students, and transgender or non-binary students will consistently be unable to be identified by FR (Scheuerman et al., 2019).

Similarly, the Aadhaar biometric identification system discussed in the previous section has disproportionately hurt India’s minority groups. Registration for Aadhaar is mandatory and failure to do so could result in exclusion from nearly all activities in day-to-day life. However,

many of India’s citizens, from manual laborers to leprosy patients, have damaged fingerprints or eyes and therefore cannot register with the Aadhaar system (Goel, 2018). This renders these groups unable to access all of the services that Aadhaar’s biometric identifiers gatekeep. This can result in extreme deprivations, because Aadhaar controls access to food rations and welfare. In the northeastern state of Jharkand, 20% of households were unable to get their food rations—more than five times the failure rate under the old system (Goel, 2018). The sad irony is that the exclusive nature of this technology renders the people who most need Aadhaar to work for them—that is, laborers, the sick, and the undocumented, who are all more likely to be welfare recipients—the most likely to be excluded from the system and all of its benefits. In this way, the design of Aadhaar harms certain citizens by rendering them invisible to the technology, thus depriving them of services.

Altering Behaviors to Avoid Surveillance

In the face of surveillance, subjects will often attempt to alter behaviors in order to maintain some privacy. This can have detrimental effects. In localities that use predictive policing algorithms, citizens often try to avoid areas with increased law enforcement presence (Brayne, 2014). They are also reticent to provide identification data that could get shared with police, though this sometimes means that they forego fundamental necessities like banking and healthcare. This is clear in the case of children who are undocumented or whose

parents are undocumented. Many studies have established that fear of police and fear of immigration enforcement places constraints on nearly all aspects of the lives of undocumented people, including accessing healthcare (Hacker et al., 2011), sending their children to school (Dee & Murphy, 2019), or even leaving the house at all (Lopez, 2019). When there is a visible police presence in a given location, undocumented people are likely to avoid that location; when that location is a school, undocumented parents are likely to be less involved in their



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

childrens’ education and school community. This example shows that when subjects of surveillance attempt to resist it, they can be excluded from important services. This can harm them and their families. We expect that, because FR in schools will enact a similar type of surveillance, we would see students and their parents altering behaviors in order to maintain some privacy. This will result in their exclusion from important services.

Conclusion

Like the other technologies discussed in this section, FR could create a narrow definition of the “acceptable” student and exclude and punish those who don’t fit that standard. Like CCTV, Aadhaar, and predictive policing, FR privileges some subjects over others. It is more likely to accurately identify white, cisgender, abled students than non-white, gender non-conforming, or disabled students (Buolamwini & Gebru, 2018). In addition to this technical exclusion of students who fall outside of FR’s “norm”, students who fall outside a school’s definition of acceptability will be hypervisible and potentially subject to punishments that would not have occurred in the absence of FR. School administrators may use FR to identify and punish students who they deem to be dressed inappropriately—a punishment that may have not occurred in the absence of this technology.

FR’s potential exclusion of certain groups could have many negative effects on students who do not fit the definition of “the acceptable student”, including more frequent punishment and creating barriers for students to pay for lunch, gain access to certain rooms or resources, and check into class. These students might either be unable or unwilling to participate in school activities as a result, which could degrade their educational experiences and opportunities. In sum, we expect that FR in schools will exclude and punish students who fall outside of a specific definition of “the acceptable student”: this will likely include students who are minorities, undocumented, gender non-conforming, and disabled, as well as students who express themselves in ways deemed inappropriate by administrators. This will have the effect of degrading these students’ educational experiences and sense of belonging at school.

Creating New Commodities and Markets

KEY TAKEAWAYS

- FR in schools will generate new kinds of student data that will be sold and bought.
- FR systems will normalize the collection and commodification of student data, creating a culture of permissiveness and teaching children that it is normal to give away biometric data and have it used to track location, purchases, and activities.
- It is very difficult for FR systems in schools to gain meaningful consent from students, because they know little about how the technology and data will be used and because consent forms are too long and technical. Furthermore, it will likely be impossible to opt-out of the system completely.
- In the past, people have had limited success in asserting ownership over their data.
- Without strong regulation, data collected for one purpose will be used in other ways.

FR in schools will generate new data on students, including but not limited to their images and movements. Previous experiences with similar data-generating technologies suggest that providers of these technologies will seek to commodify this data, adding questions of ownership, value, and even market exploitation to the concerns we have discussed throughout this report.

Governments, researchers, non-profit organizations, and industry have long collected data from the world's citizens, from biological and health information to census data. Technologies such as blood tests and

online applications have facilitated this data collection, and in recent years it has gotten easier to store, classify, and process large amounts of data. Organizations are now assembling large databases, often pulling together different types of information, in order to characterize populations and make predictions about their needs and behaviors (Linder, 2019; Sankar & Parker, 2017). These databases become major sources of value, and in some cases organizations have begun to assert intellectual property rights on or sell access to them (Linder, 2019; Ciuriak, 2018; Turner et al., 2013). As we discuss further below, individual citizens have had

limited success asserting ownership over their data: while citizens have occasionally forced the entities collecting and processing data to value their ownership through public shaming campaigns, or by simply preventing access until a benefit-sharing agreement is made, generally courts have not been sympathetic to their claims.

Meaningful consent is often limited by 1) the lack of other available options for a service, as in the case of school, 2) asymmetric information between the organization and the individual that obscures the value of the relinquished data, as when human tissue is donated to research, or 3) by complicated consent forms that are too long and technical to be meaningful to users. All of these factors are at play with facial recognition in schools, and students are further at risk from systems that are not equipped to protect their data even when they agree to the terms of collection.

Companies Will Expand Surveillance to Gather Data

Companies have the incentive to expand the reach of surveillance technology as much as possible because they can monetize data they collect by building new products or selling the data directly. While data does not have a stable value, it has become a lucrative business for the companies who aggregate and sell it. Meanwhile, the human sources of that data receive little direct remuneration. For example, in return for access to in-kind services such as email or social networks,

users provide data which is then repackaged and sold to companies who use it for targeted advertising, to develop or improve services, to assess customer risk, or to disincentivize customers from leaving the platform (Zuboff, 2018). In 2017, researchers valued the services that consumers got in exchange for their data at about \$300 billion, but companies earned trillions of dollars annually by aggregating, selling, and processing the data (Nakamura et al., 2017). Evidently, the data business is a highly profitable one.

Google's parent company Alphabet, for example, makes most of its money from the data it collects and sells to advertisers from those who use its free services (Forbes, 2019). Google uses its large network to combine data collected across many contexts, including customers' offline lives using phone application data (Ciuriak, 2018). It stores all of this information in a single database called Sensorvault, which increases the value of the information to the company and has the side-effect of making it easy for police to use subpoenas to gather a lot of information quickly on Google customers (Valentino-Devries, 2019).

We see this trend among FR companies as well. Vigilant Solutions began as a standard service company, but has built a database which it now sells to law enforcement (Linder, 2019). The company first sold license-plate tracking technology to private clients. Together, these cameras generated data in real time about car movements. To monetize that data, Vigilant sold law enforcement access to the licence-plate information in a package with software that

integrated information from other publicly available data sets. Vigilant's database is so valuable that the company now gives away the camera hardware for free so that it can expand its pool of data, which has resulted in over 13 billion license plate detections in the US with over 250 million new plate captures (with location information) per month.

To facilitate data collection, Vigilant established its proprietary LEARN cloud database in which customers upload their data for analysis. In the process, they encourage law enforcement departments to share data with one another, and many do. This network of data sharing within the pay-for-access cloud is an added incentive for potential customers to use Vigilant over another policing platform, making it difficult for new companies without existing networks of customers to compete and enter the market (Ciuriak, 2018). Vigilant also now integrates FR and public data (Linder, 2019). After entering the education market, the company encouraged local departments and school security teams to share data in LEARN and coordinate efforts, which could lead to increased police participation in security activities that are traditionally handled by schools. In the process they are increasing the value of LEARN, which will likely create more revenue for Vigilant.

If FR companies have access to student data, they are likely to find ways to monetize it, as Alphabet, Vigilant Solutions, and countless other technology companies have done. This could encourage companies to advocate for expanding surveillance systems to new schools and for new uses in existing schools

to generate more data, all without adequate consent.

Once Collected, Data Can Be Repurposed

In the absence of strict regulation, data collected for one purpose can be used in other ways. These alternate uses may come into play as new needs arise, as technology changes, as organizations develop new ways to extract more value from the data, or when access to the data is transferred to a new group. Often the additional uses are not subject to the same level of scrutiny as the original stated use, even though lawmakers would likely not allow the new uses if they stood alone, and users, like early customers of the Vigilant Solutions license plate reader, might not want to give data for this new purpose. Further, rather than a potential use driving new data collection and analysis, available data simply gets repurposed for new uses whether or not it is relevant. This is problematic because the data is often opaque to end users and they don't realize that its use has been redirected. And these mismatches can be consequential when used by government or law enforcement. Law enforcement departments are a common secondary user of data collected by other entities know this, but users may not.

One example of data that is repurposed after collection is Google and Ancestry.com data (including user location, photos, and DNA tests) that is collected for commercial purposes but is ultimately used by law enforcement. Law enforcement offices

in the United States, for example, have begun to request or get warrants for access to their databases, which are useful for solving crimes. Police have long subpoenaed information from Google's database to investigate individuals for whom they have already established probable cause. This includes information about search history,



Flickr user Torkild Retvedt, CC BY-SA 4.0

email data, and phone location (Valentino-Devries, 2019). In 2016, police also began subpoenaing data based on location. This meant that they could gather information from a particular place at a particular time, if they had reason to believe a suspect for a known crime would have been there. This vastly expanded the information they received, as well as the number of people caught in their dragnet. Similarly, police recently served Ancestry.com a warrant to search the company's database of DNA tests. Prior to the request, police could access GEDmatch, a smaller database, but the forensic technique that leverages DNA information is more successful with

a larger database of DNA and genealogical information (Aldhous, 2020). While users would likely not have shared their information with law enforcement directly, or allowed law enforcement to create similar databases through a vote or local government ordinance, once the companies gathered the data it became available for these purposes. This makes clear that once data is collected, it can be repurposed for uses that the subject didn't consent to.

This suggests that once schools collect FR data for any reason, the data will be available for other uses that parents and local officials may not have approved. For example, a school could install FR to identify students for school lunches, but later use the data to identify and discipline students who are not following the dress code. Even if FR companies do not explicitly share data with law enforcement, by using the systems, schools will generate new data that police may be able to access down the line: for example, information on the whereabouts of undocumented parents who visit schools to participate in their child's education.

Do Citizens Own Their Data?

There is limited legal or policy clarity on the question of whether citizens own their data, anywhere in the world. But state-level cases from the United States suggest that at present, the answer is no (Gotwalt, 1992). The first such case was *Moore vs. Regents of the University of California*, decided by the California Supreme Court. In 1987, the

University of California Los Angeles Medical Center treated John Moore for a rare form of leukemia. Dr. Golde, Moore's physician, noticed that Moore's blood had properties that made it medically valuable to research. Dr. Golde continued to take samples from Moore throughout treatment and contrived follow-up appointments to be conducted exclusively at UCLA, even though Moore lived in Seattle, to prevent other labs from gaining access to Moore's bodily materials. Dr. Golde used the blood and tissue samples to develop a useful new cell line, patented it and other discoveries that followed, and struck valuable licensing deals with private companies for access to the line. Moore was not notified that this research was occurring, nor asked to sign a consent form until after Dr. Golde had filed his first patent application. When he discovered this use, Moore sued both Dr. Golde and UCLA. He argued that he did not consent to how his blood and tissue samples would be used and that he had a property interest in his cells. In its decision, the California Supreme Court determined that Dr. Golde had a duty to tell Moore about the research and the potential profit that it might generate, but that Moore did not have a property right to his tissue either while it was inside him or after it was removed, because he had essentially discarded it (*Moore v. Regents of the University of California*, 1990). The US Supreme Court did not weigh in.

In making this decision, the California court acknowledged previous legal opinions which held that everyone has a proprietary interest in their "own likeness" and that individuals can bring a civil lawsuit for "unauthorized, business use of a likeness" (*Moore v. Regents of California*, 1990). But, it noted that these decisions did not link this interest to property law; in fact, previous courts had said it was "pointless" to debate how to properly characterize the property interest in a likeness.

Similarly, years later a group of parents sued Dr. Rueben Matalon and the Miami Children's Hospital Research Institute, for taking their children's DNA and using it to develop a lucrative genetic test for Canavan Disease

The California Supreme Court determined that Dr. Golde had a duty to tell Moore about the research and the potential profit that it might generate, but that Moore did not have a property right to his tissue either while it was inside him or after it was removed.

(Greenfield, 2006). The parents had provided the information with the understanding that it would be used to develop a test that would be widely available to affected families, and were distressed when Miami Children's Hospital charged high prices. But as in *Moore*,

the Florida court ruled that the plaintiffs did not own their tissue samples. Any litigation over ownership of FR data is likely to refer to this case history, making it difficult for plaintiffs to establish ownership in their images and related data. However, judges in the *Moore* case also weighed the plaintiff's property interest against "medical research of importance to all of society", concluding that this medical research created a strong justification for using Moore's cells. FR providers would not be able to claim such a strong justification for using subjects' data without consent.

It is unclear whether FR providers have attempted to patent the biometric data they have collected or generated, but like other data providers, most have created private databases with this information and then sell access to this information. They then distinguish themselves in the market by suggesting that the size of their databases improve the accuracy of their technologies (Hill, 2020a). To date, court cases brought by consumers against technology companies over biometric data ownership have focused on consent and privacy rather than data ownership. However, courts in the US have used these privacy cases to comment on ownership, and have largely maintained the stance established in *Moore* that consumers have no property rights over their data unless they can show that they had planned to use or sell the data themselves (Elvy, 2018). It is likely that ownership challenges will emerge both in the United States and elsewhere as the use of FR expands.

Data Authorization Focuses on Consent, Not Ownership

While the courts have been reluctant to acknowledge that citizens have property interests in their biometric data, they do emphasize full, informed consent. This framing has been reinforced by the dozens of "biobanks" (combined storehouses of genetic, health, lifestyle, and other data related to individuals) that scientists and governments have created over the last few decades.

Biobanks are repositories of biological samples, from tiny "blood spots" taken from newborns to tissue and DNA samples taken from communities. They may be linked to other forms of data, including personal and family medical history and environmental information. Scientists, physicians, and public health officials hope that by pooling this information, they can develop a systematic understanding of the relationship between DNA, the relative roles of an individual or community's genetic makeup, and environmental and lifestyle factors on disease risk. Most biobanks frame the collection and use of biometric data in terms of donation and consent rather than ownership of data.

However, there are many different types of consent frameworks (Steinsbekk et al., 2013). Since scores of studies may be conducted with the data from a single biobank, by a variety of researchers, it is easiest and most

common to have a blanket “opt-in” policy, meaning that the individual consents to any and all research conducted using their data (Denny et al., 2019). Most biobanks with this policy allow individuals to withdraw consent at any time. But some suggest that individuals should be allowed to provide “dynamic” consent, making individual decisions about participation in each project (Prictor et al., 2018). Advocates in consumer technology have gone further, adapting a prominent consent framework that gives subjects more power, advocating that consent should be freely given without pressure or manipulation, reversible at any time, informed by an honest and clear explanation of possible uses and protections, enthusiastic rather than coerced by the withholding of services, and specific to the uses described (The Consentful Tech Project, n.d.). These different frameworks could be useful for designing FR consent policies.

Due to the nature of FR tools, which are often designed 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. Rulings in Europe against school-based FR systems, as well as against Facebook’s FR system, suggest that in a data protection scheme that emphasizes consent such as the General Data Protection Regulation (GDPR), applications of FR will necessarily be limited to systems in which each individual must opt in (Kayali, 2019). The US does not currently require individual

consent for FR at the national level, although some states do have GDPR-like restrictions such as the Illinois’s Biometric Information Privacy Act (Todd, 2020). Furthermore, in the context of education, while the Federal Educational Rights and Privacy Act (FERPA) formally has a consent model, it delegates consenting authority to schools, with no individual remedies if schools authorize the use of a tool or platform that is later found to violate students’ privacy (Zeide, 2017). The only available consequence for an institutional violation of FERPA is that the federal government may withhold funding, but that consequence has never been applied. Ultimately, there appears to be few, if any, policy or legal tools available to remedy consent violations in schools. If parents, guardians, or students object to a school’s use of a technology such as FR, they have had to rely on political pressure rather than FERPA.

... despite strenuous objections by parents and an investigation by the New York State Education Department, the state allowed Lockport, New York’s school district to roll out FR in January 2020.

And often, political pressure is not effective at preventing school FR use. For example, despite strenuous objections by parents and an investigation by the New York State Education Department, the state allowed Lockport, New York’s school district to roll

out FR in January 2020 (Alba, 2020). After the New York Civil Liberties Union filed a lawsuit, the state assembly signed a law enacting a moratorium on the use of biometric identification technologies in schools (New York Civil Liberties Union, 2020). At the time of this report, the bill is awaiting approval by the governor.

Companies usually need information from many users in order to monetize data as described above, but there is no mechanism for group consent. In fact, FR companies may pool data from multiple schools to create powerful tools, compounding the value of data from each person. However, consent is an individualized process and does not consider how that data takes on greater meaning when combined with others. Further, in countries without biometric data protection policies that explicitly address this issue, students give no consent at all. Evidently, there are multiple barriers to obtaining meaningful consent from students for FR to be used in their schools, raising concerns that any use of this system will be without the consent of its subjects.

Limited Data Protections Put Privacy at Risk

Previous surveillance technologies have also created a culture of permissiveness around data, leaving young people vulnerable to unauthorized use of their personal information. By making FR a routine part of life at school—particularly without any explicit discussion about where and how to release this data—students may learn that

it is unremarkable to give away biometric data and have it used to track your location, purchases, and activities, which could set them up for a lifetime of participation in data collection programs prone to leaks and hacks.



Flickr user Fotokannan / CC BY-SA 4.0

Architects of India's Aadhar initiative, launched in 2009, hoped that it would reduce corruption and fraud, increase efficiency, save taxpayer money, improve provision of government programs, and bring all citizens—including rural or impoverished citizens who have been historically excluded for not having the necessary documents to prove their identities—into the digital age (Goel, 2018). However, the program has had major security lapses, rendering Indians vulnerable to theft and abuse of their personal biometric information. In 2017, an investigation by *The Tribune*, an Indian newspaper, found that reporters were able to access names, contact information, and postal codes after paying an individual linked to former Aadhar employees the equivalent of eight US dollars (Doshi, 2018). For another five dollars, reporters could receive printed

out copies of others' Aadhaar cards that they could use to impersonate them and access government services (Doshi, 2018). Additionally, in 2017, 210 government websites leaked Aadhaar data including names, birthdates, addresses, bank account numbers, and ID numbers of millions of people (The Hindu, 2017). Some of this data can still be found easily online (Goel, 2018). This is just one such data breach—over the years others too have exposed the biometric, personal information of millions of Indians (Jain, 2019). Breaches like these are particularly problematic because victims will experience the effects of a leak for the rest of their life, as one can never change their fingerprints or iris scans like they can a leaked password (Perrigo, 2018).

Aadhaar shows us that it can be challenging to implement data protections robust enough to safeguard subjects' sensitive personal data, and that failure to do so can result in security breaches that have harmful consequences for users for the rest of their lives. If the Indian government is unable to adequately protect this sensitive data, it certainly raises questions about whether local school districts

will be able to, and the extent of privacy and data security risk we may expose students to by implementing FR systems in their schools.

Conclusion

History suggests that organizations will find ways to commodify FR data from schools, raising questions of market exploitation and student consent. It is difficult for students, teachers, and other visitors to schools to meaningfully consent to FR because they do not have alternate options to attending school, they may not understand the potential uses of FR, and they may not know what they are consenting to or how to opt out. Ultimately, it seems that instituting FR in schools opens up students to their data being commodified and either sold or stolen without their knowledge and consent. Not only does this invade student privacy and compromise their sensitive data, but it also creates a culture that teaches students that it is normal and unremarkable to give away sensitive information. For these reasons, we strongly advise against the implementation of FR in schools.

Institutionalizing Inaccuracy

KEY TAKEAWAYS

- FR codifies human judgments and biases and it is almost impossible to achieve complete accuracy.
- Facial recognition is much less accurate in identifying people of color, children, women and gender non-conforming people, and disabled people.
- Because it is technical, people assume FR is unbiased. This makes it harder to challenge. However, FR codifies inaccurate and racist human biases and amplifies their potential damage by expanding the reach of surveillance.
- Proper FR system maintenance requires extensive resources and staff training. Schools are unlikely to keep up with this maintenance, rendering the results not only meaningless, but dangerous.
- Seemingly simple technological solutions are often quickly entrenched. It then becomes difficult to identify and address problems.

Even if a school determines that the potential benefit of using FR outweighs the costs outlined in the previous sections, the technology would need to be accurate in order to be useful. That is, it must be able to detect and identify faces correctly. However, the analogical cases of CCTV, predictive policing, and the breathalyzer, among others, teach us that establishing and maintaining accuracy is exceedingly difficult and sometimes impossible. While technologies tend to be perceived as objective, and therefore free from bias, in reality they are influenced by the humans who make and use them as well

as the norms, institutions, and laws that govern their applications. Proponents of the technology might point out that even if FR is only as accurate as humans, automated surveillance systems are more efficient, and can therefore create more benefit. However, it is important to remember that this means they can also expand the reach of the bad effects of biased surveillance. This means that more students will experience the harms discussed above. And, given the history of surveillance technologies we detail in this section, FR will likely amplify significant problems of misidentification.

FR is Inaccurate Among Most Populations, Including Children

FR's inaccuracy begins with data collection and algorithm training processes. As discussed in the Introduction, FR algorithms are first developed using a "training" data set of facial images. The FR system learns how to read faces by taking multiple measurements from the images in this data set, such as the distance between eyes and the length and width of the face (Thorat et al., 2010). It then learns to match images, identify demographic information, or detect particular emotions. Training sets include labels that provide this information, so algorithms learn which characteristics and measurements correspond to each label. However, the quality of the algorithm depends on the representativeness of the training data set. If a data set contains only white faces, for example, the algorithm will only learn the measurements that make up a white person's face image, which could include shadows and contrasts that may not be as prominent in non-white skin tones. This could produce inaccurate measurements and ultimately, incorrect matches for Black and brown faces. The same is true for differences in gender, age, and disability status. However, these inaccuracies can be difficult to uncover. When an FR provider promotes its high accuracy rates, users must be careful

to determine whether the data set used for training matches the population they hope to track. Otherwise, the statistics are meaningless.

While we have little public information about the demographics of FR training data sets, studies suggest that most are not representative. As a result, they will pose significant problems for widespread use. An MIT Media Lab study found that facial recognition systems were as much as 40 times more likely to misidentify the gender of a dark-skinned woman as a white man, and attributed the problem to demographically limited training sets (Buolamwini & Gebru, 2018). FR systems are also two to five times more likely to produce a false positive identity match in women than men, depending on the particular software (Grother, Ngan, & Hanaoka, 2019). The most common FR testing data set is 77.5% male and 83.5% white (Han

FR will be much less accurate among children since their faces change so quickly and differ significantly from one another, in comparison to variation among adults.

& Jain, 2014). Furthermore, NIST, which tests FR systems in the US, has not disclosed information about the demographic makeup of its data sets (Gates, 2011). Therefore, it is difficult to contextualize the accuracy

statistics it reports. When NIST built a new database specifically to determine whether facial recognition technologies could identify gender equally well across racial groups, for example, it used country of origin as a proxy for race and did not include any countries that are predominately Black (Buolamwini & Gebru, 2018).



State of Maryland, CC BY 2.0

FR will also be much less accurate among children, since their faces change so quickly and differ significantly from one another in comparison to variation among adults (Grother, Ngan, & Hanaoka, 2019). The faces of growing children cannot be easily compared to static training sets. If schools use reference pictures that are more than a year old, or try to apply these technologies to younger students that are growing rapidly, facial recognition will not work well. Most of the images in FR databases are from people between the ages of 20 and 60 years old. But to capture the high amount of facial variation both between children at young ages and between children and adults, children need

to be overrepresented (Han & Jain, 2014). Providers will likely advertise statistics about their system's accuracy based on its use among adults; schools must be careful to demand accuracy measurements for the technology's use among children before purchase.

As detailed in previous sections, FR will disproportionately impact non-white, disabled, non-male students. It is also particularly bad at identifying children, which presents obvious challenges for use in schools, including the potential for an abundance of false matches and false reports that, at best, render the system not only burdensome but potentially unusable. Despite evidence to the contrary, proponents of FR in schools, including the companies that sell the technology, are likely to claim that the systems are unbiased simply because they are more technically sophisticated. Unfortunately, this argument may resonate with those who do not understand algorithm development.

Humans Make Final Matching Determinations

Even if governments regulate the accuracy of face-matching algorithms, FR technology will always involve a final check by a human being. This human check will introduce additional biases. Research on “forensic confirmation bias” has shown that when there is uncertainty in the process, forensic examiners tend to focus on evidence that confirms their expectations, while ignoring information that does not (Kassin et al., 2013).

We have already seen this problem in the case of CCTV. First, camera quality is a problem; schools may use low-quality CCTV cameras and the frequency of camera updates varies considerably across schools and countries. Second, when camera quality is poor, even trained observers perform at less than 70% accuracy (Lee et al., 2009). Camera quality is likely to continue to be a problem with FR, since many schools will likely rely on their existing camera networks and simply add FR software to analyze the images. Also, observers often have difficulty detecting whether a crime even occurred at all, even when quality is not an issue (Keval & Sasse, 2010). Notably, these studies have used white subjects, and researchers have not repeated them with other groups to determine the accuracy of human checkers in identifying people of color.

But we already know that average eyewitnesses struggle to correctly identify people of a different race in comparison to same-race identification (Hugenberg et al., 2010). While it is impossible to know the actual rate of mis-identified suspects, we know that those who were exonerated using DNA had often been incarcerated based on eye-witness testimony by people of other races (Scheck et al., 2003; Smith et al., 2004). In one study, at least 36% of overturned convictions involved cross-race identifications (Scheck et al., 2003). This could amplify the racial bias already embedded in FR training data and algorithms.

We also see how human interpretation can vary in the case of fingerprinting. As with FR, fingerprints can look very different

in reference databases than they do when police capture them for forensic analysis, because fingertips are soft and can warp on uneven surfaces or with different pressure patterns. In fingerprint analysis, software will suggest a number of matches, and fingerprint examiners examine the ridge patterns to confirm matches to the prints of interest (Kruse, 2005). Unfortunately, not only can different examiners looking at the same prints come to different conclusions, but even the same examiner looking at a print multiple times can draw different conclusions each time (Cole, 2003; Ulery et al., 2012). A survey of research on fingerprinting analysis found that even in studies designed to eliminate contextual information that might lead to cognitive bias, examiners incorrectly identified matches (false positives) in between 0.17% and 4.2% of fingerprint pairs (President's Council of Advisors on Science and Technology, 2006). In studies that observed examiners in their typical operating contexts, Federal Bureau of Investigation (FBI) researchers found they tailored their documentation to support their preliminary conclusions, rather than making a determination based on the examination (Ulery et al., 2014). While research has not evaluated whether information on race specifically influences fingerprint determinations, examiners are influenced by other information, such as the opinion of other experts and suspect confessions (Dror et al., 2006). Again this has disparate impacts as false and coerced confessions are more common among non-white populations (Villalobos & Davis, 2016).

An example in South Wales illustrates the typical procedure for a human check on FR

results (though this procedure can differ across departments and processes are often opaque). The South Wales Police use FR in real time at events to look for anyone who is on their watchlist. If the software flags a face as a “match”, a police officer who has been designated an “Automated Facial Recognition” operator verifies the finding. If the operator believes that the match is correct, they tell another officer who is on location. The officer on location also judges whether they believe that the match is correct, and is only supposed to intervene if they agree with the finding (*Bridges, R. v. The Chief Constable of South Wales Police, 2019*). FR needs a great deal of human involvement in order to function, but supporters often claim that it is more objective than other methods because it is run by algorithms. After an early deployment, the South Wales police claimed that although the algorithm falsely identified over 2,000 people, they were able to arrest over 450 people without arresting anyone who was falsely identified (*The Guardian, 2018*). However, it is difficult to identify arrests from false identifications

FR needs a great deal of human involvement in order to function, but supporters often claim that it is more objective than other methods because it is run by algorithms.

because the police control what statistics get shared, and it is important to note that false

identifications still increase contact with the police, which can be dangerous particularly for people of color, and can lead to additional charges.

Systemic Discrimination Feeds Back Into Surveillance Technology

Surveillance technologies are particularly susceptible to bias and systemic discrimination because they are part of feedback loops that encode and amplify human biases (O’Neil, 2016). Humans set up systems based on biased information such as FR training sets that under-represent minorities and police databases that represent a known history of racially biased policing. As a result, the technology’s outputs reflect these biases; but, because they are the result of an algorithm, they are considered more objective and accurate than the human findings. People then act on the results of the biased technologies, producing outcomes that appear to confirm their bias, that then get fed back into the technology, further entrenching discrimination. Because the exact workings of these algorithms tend to be protected as trade secrets, it is difficult for anyone who didn’t produce the algorithm to contest these entrenched biases, which we discuss further below.

Predictive policing, which describes any policing strategy that attempts to stop crime

before it occurs, has followed this pattern (Haskins, 2019). It is guided by the idea that there is some consistency (in terms of environment, offenders, and victims) in when and where crimes take place; if those elements can be tracked, police can predict crime (Hunt, 2019). In addition to location-based approaches, predictive policing now includes other methods that are further from the foundational theory and target individuals, types of crime, and whole communities (Haskins, 2019). This method has been used for years (in stop-and-frisk policies, for example), but today it has become more technological with the assistance of algorithms and big data.

Researchers have shown that this feedback loop leads departments to over-police certain neighborhoods, particularly in communities of color that may not actually have comparatively high crime rates (Lum & Isaac, 2016; Ensign et al., 2018). Stop and frisk increases interactions between residents and police officers, which feeds back into crime statistics as well as other criminal justice metrics, perpetuating the “high crime” categorization of the area. These communities often lack resources, so the use of predictive policing further disadvantages them (Ferguson, 2011). The Supreme Court has also permitted lower standards for police intervention on the basis of “reasonable suspicion” in “high crime” areas, reinforcing a feedback loop that functionally reduces

the legal rights of people living in these neighborhoods (Ferguson, 2011).

Algorithms also transform human biases into systems that can outlast individual events and bad actors if not carefully managed. A case study of 13 departments using predictive policing technology found that in addition to basic errors in data preparation and collection, nine trained their models using data from periods when the department had been sanctioned for illegal practices (Richardson et al., 2019). This essentially laundered illegal police practices into “legitimate” predictive data, further reinforcing unfounded perceptions of criminality in underrepresented communities.

Whether knowingly or not, police departments take advantage of the perception that predictive policing algorithms are objective (Ferguson, 2016). Both companies and media outlets refer to the systems

Algorithms transform human biases into systems that can outlast individual events and bad actors if not carefully managed.

as scientific and unbiased, and police departments have already been able to leverage this defense in court to claim that

some arrests could not have been biased because they were based on algorithmic predictions (Gorner & Sweeney, 2020). As a result, the algorithms go largely unchecked, which further limits the options for already marginalized groups to obtain justice.

While there are no similar studies on surveillance and policing feedback loops and disability, since disabled students tend to be disciplined at a higher rate (with Black disabled students facing the highest rate of all) than non-disabled counterparts, we are likely to see similar issues with disabled students and school FR systems (Alabama Appleseed, 2019).

Maintaining Accuracy Requires Sustained Resources and Training

Once adopted in a rush of technological optimism, law enforcement departments often do not properly maintain or update surveillance technologies. This reduces accuracy and utility significantly. In the case of predictive policing, rigorous testing of predictive policing systems rarely takes place after implementation (Gorner, 2016). Instead, they use informal checks that are poor substitutes, including checking if people on the predicted watch list are getting arrested or, in the case of a victim watch list, killed (Gorner, 2016). Meanwhile, although in the United States and the United Kingdom there are formal training programs for the analysts who manage this software, there are not always similar resources for the

police officers in the field who perform data collection and implement orders based on software findings (Perry, 2013; Cope, 2004; Ferguson, 2017). Additionally, it is impossible to assess the accuracy of policing software if officers do not follow up on the findings. In several studies, researchers blamed a software package's poor results on police's failure to consistently follow protocol, rather than a flaw within the software (Haskins, 2019; Perry, 2013).

In the case of breathalyzer tests (machines used to determine whether a driver's blood alcohol content is over the legal limit), best practices require dozens of hours of training and assessment per officer on an ongoing basis. The Canadian Society of Forensic Science (CSFS) recommends that officers who administer breathalyzer tests should receive at least 20 hours of instruction from certified forensic labs on topics including pharmacology and relevant aspects of physics, 31 hours of practical training that includes device maintenance and practice tests, and 3 hours of oral and written examination before they perform breathalyzer tests in the field, with at least 7 hours of refresher courses if an officer has not used a breathalyzer in 12 months (Bergh et al., 2013). Any department with over 10 breathalyzer units should also employ a full-time field coordinator. Few departments meet those standards. A 2019 New York Times investigation found that judges in New York and New Jersey had barred evidence from over 30,000 breathalyzer tests over a 12-month period after finding that the machines had been improperly maintained and calibrated by departments (Cowley & Silver-Greenberg,

2019). Given the large number of surveillance technologies, including FR, being introduced to law enforcement departments, it seems highly unlikely that police officers will be able to complete all of the necessary training. Similarly, schools that introduce one or more technologies may quickly struggle to keep their staff up to date.

The technologies themselves also require ongoing oversight and maintenance. FR systems calculate similarity scores based on the probability that two faces are the same, and depending on how a department sets the software's certainty threshold, the technology may incorrectly reject too many faces (false negative results) or incorrectly flag too many (false positive results), affecting the technology's utility and validity (*Bridges, R. v.*

The Chief Constable of South Wales Police, 2019; Amazon Web Service, n.d.) Thus, an organization using one of these systems must continually ensure that the specifications are set correctly, particularly after any updates or maintenance. Software must also be updated in order to take advantage of advances in FR technology, but current FR practices in law enforcement indicate that police departments may not always be using the most updated version of the technology. For example, a New York Times investigation found that in

2020, Pinellas County, Florida was still using a FR system last updated in 2014 (Valentino-DeVries, 2020). Schools may not be able to afford the latest technology, which would prevent their systems from improving even as the rest of the field advances.

FR will be an ongoing financial and human capital burden for schools that are already often underfunded and understaffed. If administrators fail to dedicate significant resources on an ongoing basis to maintaining software systems and entering new data from incidents, visitors, and new or aging students, they may quickly find that their systems are no longer as accurate as they might have been at installation. Even if they are able to keep up with this demand, identifying problems alone will not be sufficient to create change.

FR will be an ongoing financial and human capital burden for schools that are already often underfunded and understaffed. If administrators fail to dedicate significant resources on an ongoing basis to maintaining software systems and entering new data from incidents, visitors, and new or aging students, they may quickly find that their systems are no longer as accurate as they might have been at installation.

The schools would also need clear guidance on how to respond to an alert from the system and consistent follow-through, which may prove difficult, particularly if FR is used to identify rare security threats.

Difficulty of Assessing Accuracy in Preventing Low-Probability Events

Proponents of FR in schools argue that the technology will prevent school shootings and terrorist attacks. But, because these events are statistically so rare, researchers would not expect to see many such events over the course of a given observation period. This creates a measurement challenge in determining the effectiveness of FR technology (Fussey, 2007). In order



exacq

to overcome this measurement challenge, observers would need to look over a long period of time or in many locations to

determine if FR actually prevents school shootings or terrorist attacks, but even in doing this it would be difficult, if not impossible, to attribute any change in school shootings or terrorist attacks to the implementation of FR technology. The difficulty of assessing the accuracy in preventing low-probability events therefore means that it is also difficult to assess the effectiveness of FR systems in schools.

Local Officials Must Determine Accuracy Among Heterogeneous Products

In the absence of regulation at the national or state level, decisions about which technologies to purchase and use are often made on an ad hoc basis by local officials, who usually lack the expertise to understand how the technology might or might not work, how to maintain and use it, and even what questions to ask. And the technologies available can be multiple and bewildering. For example, the data and algorithms used for predictive policing differ in key ways across products. The popular service PredPol uses only anonymized data on crime and location to predict areas that are likely to experience certain types of crime at specified times, while Palantir's predictive policing system also identifies high risk individuals (Ahmed, 2018). But, these differences may not be clear to users, and users may not have the expertise to ask about these technical specifications when making decisions about what to purchase. Also, they may not know

how to judge the effectiveness rates provided by the company. Often, the “control” group in assessing effectiveness and cost metrics are not “treatment naïve”. This means that, rather than comparing departments that use data to predict crime with departments that do not, effectiveness rates make comparisons between the predictive performance of humans and algorithms. To compound the issue, FR companies have been caught making false or misleading claims in their sales and marketing materials (Snow, 2020).

For example, we already see significant diversity in the FR technologies that providers are offering to schools, which could make it difficult for untrained school administrators to make decisions about these products. Secure Accurate Facial Recognition (SAFR), offered by Real Networks, allows people to unlock doors with their face instead of an identification card or passcode so the tool can be used as both a form of security and identification (SAFR, n.d.). The service does not have a cloud-based sharing platform, and does not seem to draw information from any databases provided by the company, but instead requires schools to build their own databases of students, staff, and visitors, and code them with threat levels and permissions (SAFR, n.d.). Vigilant Solutions’ FR product, by comparison, runs the analysis of identified faces in their LEARN cloud database, where schools can share and use information from local police departments and public databases (Linder, 2019). In order for school districts to understand the relative benefits and risks of these technologies, and even how to use them properly, they will need the expertise to evaluate and monitor them.

Limited Regulation of Surveillance Technologies

Surveillance technologies go surprisingly unregulated. For example, even though the results of a breathalyzer test can lead to fines, jail time, and a revoked driver’s license in the United States, the devices are exempt from regulation by the Food and Drug Administration (FDA) and do not need to undergo formal testing or independent verification before market entry or police use. This means that the companies can change the design at any time without testing (Food and Drug Administration, 2020).

States may choose to regulate these tests, but standards vary. Not surprisingly, then, breathalyzer results are littered with errors from flawed software, misinterpretation, and poor maintenance (Cowely & Silver-Greenberg, 2019). For example, Mississippi uses a breathalyzer device that was evaluated and determined to be flawed by Vermont (Cowely, & Silver-Greenberg, 2019). Also, when courts in New Jersey and Washington allowed prosecutors to examine breathalyzer device codes for two different devices, they found errors that the court determined could cause false results (Cowely & Silver-Greenberg, 2019). There is also no oversight to ensure that police departments set accuracy standards at an acceptable level. Furthermore, breathalyzer companies shield their products from investigation by claiming their algorithms are trade secrets and therefore cannot be shared for examination. The lack of oversight of these devices reduces

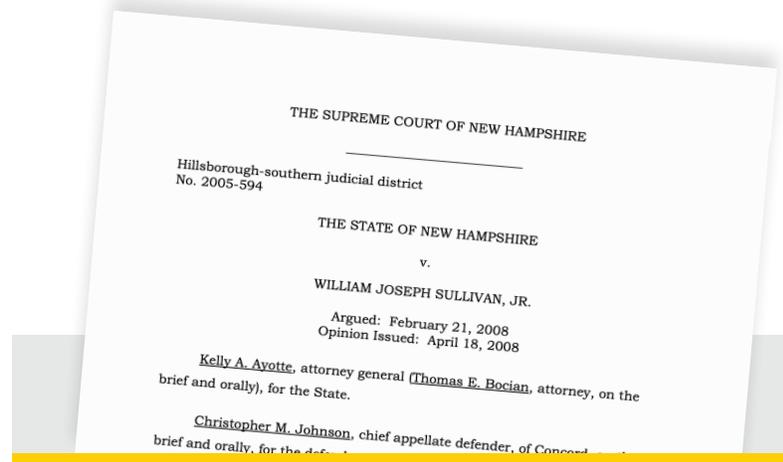
incentives to prevent flaws in their design (Levine, 2007; Short, 2007). Without oversight and expertise at the government level setting standards and enforcing compliance, most schools and districts will not have the technical resources to evaluate companies or the political or legal resources to investigate errors or demand better products.

Courts Become Ultimate Arbiters of Accuracy

In the absence of regulation, criminal courts play a central role in determining a forensic technology's acceptability (Kruse, 2016). In the United States, trial judges in federal courts and most state courts use the Daubert Standard to determine whether an expert witness' testimony about a forensic technology is scientifically valid for the case (Cole, 2003). This rule considers five factors including known or potential error rate, the existence of a maintenance standard, and topics covering reputation in scientific communities and the other measures of testing rigor (*Daubert v. Merrell Dow Pharmaceuticals Inc.*, 1993). However, the standard does not include minimum criteria for any evaluation category. Instead, for each application of a forensic technology, courts are left to determine the combination of factors that rise to an acceptable level of certainty for inclusion in testimony.

In practice, this means that a technology's accuracy is debated *de novo* in each case. While federal courts have determined that fingerprints, for example, do not meet the Daubert standard, they still

allow prosecutors to present it as "clinical opinion," which jurors may not recognize as a lesser designation (Cole, 2003). At the same time, state courts have allowed fingerprint testimony to be considered expert scientific testimony, while holding that challenges to the technology's objectivity could only be used to litigate the "weight and credibility of the evidence," not whether it can be presented in court (*The State of New Hampshire v. William Joseph Sullivan, Jr.*, 2008). Evidently, there is not a lot of consistency regarding the use of different types of technology in court expert testimony, suggesting that courts are not wholly reliable arbiters of accuracy.



As a result, the technology's accuracy is ultimately determined in the legal system by the quality of the lawyers and experts involved in a given case. This could result in essentially two separate standards of evidence for those with the means to mount a strong legal defense and those without such means. Further, law enforcement may still have the incentive to use weakly

supported technology, or technology with high error rates, if it holds up in the typical court case. FR in the school setting will lead to a similar division between students who have parents and guardians with the time and means to advocate their rights or push back against the school, and those who do not or whose parents lack social status. This will likely be another division along racial and economic lines that negatively affects the educational outcomes of students of color and economically disadvantaged students.

Excitement Over a Technical Fix Leads to Entrenchment

Technology invariably brings optimism with it: the hope that a simple technical fix can solve a complicated problem. This can lead to an over-reliance on a technology, long after the limitations on its utility has become clear. As a result, surveillance technologies like FR can become, in essence, “security theater” (Kline, 2008). CCTV, for example, is

widespread in the UK, though it rarely deters crime (Gill et al., 2005). An analysis by the UK Home Office of 14 case studies on CCTV only found 2 instances in which installing the cameras significantly reduced crime, and in both cases the cameras were in parking lots and the crime was merely displaced to another location (Gill et al., 2005). Meanwhile, police departments emphasize its successes, but don’t share details on failed procedures (Fussey, 2007; BBC News, 2017). Not surprisingly, then, public support remains high (Spriggs et al., 2005; Webster, 2009). Airport security measures are similar: their effectiveness is difficult to ascertain (Goldstein, 2017). Meanwhile, governments tend to emphasize the successes while remaining silent on the failures or even the accuracy of these measures in comparison to other techniques (Bronskill, 2012). As a result, citizens continue to believe that these technologies are vital to protect our safety, even in the absence of evidence.

We could easily imagine FR having similar power, especially when used in schools.

Because they would do anything to keep their children safe, parents and guardians are vulnerable to both companies and schools who have an interest in emphasizing the effectiveness of the technology. They may assume that because FR is new and high-tech, and because the school may release information about FR’s effectiveness and omit information about its failures, it is effective. They may not know what questions to ask in order to increase transparency about accuracy.

Because they would do anything to keep their children safe, parents and guardians are vulnerable to both companies and schools who have an interest in emphasizing the effectiveness of the technology. They may assume that because FR is new and high-tech, and because the school may release information about FR's effectiveness and omit information about its failures, it is effective. They may not know what questions to ask in order to increase transparency about accuracy.

Conclusion

At first glance, the accuracy of FR technologies seems straightforward and robust. But our analysis suggests that its limitations will be difficult to overcome. First and foremost, humans and social systems, along with their biases, are involved in every step of the FR process. Humans create the data that are fed into the algorithms, and this data tends to be racially biased. Humans create and maintain the algorithms. Humans

purchase the technologies (often with limited information about their capabilities), interpret the face matches, and maintain the surveillance systems. This human involvement matters because we have learned that the operators of these technologies often have minimal sustained training or resources to correct their biases, and the surveillance technologies themselves are subject to limited external oversight. As such, there are few checks on human judgments in these systems. The lack of oversight also gives technology providers more power to influence local decisionmakers. And even when providers are transparent about the data and algorithms they use, this information can be hard for decisionmakers to interpret (Kolkman, 2020). Finally, even if it were possible to enhance the accuracy of these technologies, it would be difficult to assess whether the security benefits outweigh the drawbacks we discuss in the other sections because the events we hope to prevent are very rare.

National and International Policy Landscape

KEY TAKEAWAYS

- No policies anywhere specifically regulate the use of FR technology in schools.
- The FR policy landscape is piecemeal across the United States and the world. Many nations and US states have proposed FR policies that have not yet passed.
- Many countries are trying to expand their FR infrastructure, without regulation.
- We classify FR policy into five types: bans and moratoria; policies mandating consent and notification; data security policies; policies that tailor the use of FR; and oversight, reporting, and standard-setting policies.

The FR policy landscape is piecemeal across the United States and the world. No country has national laws that focus specifically on regulating FR technology (or, for that matter, FR in schools). At best, countries include biometric data as a type of protected personal information in their national privacy and data laws. However, some US states and municipalities have instituted policies to provide regulatory clarity on how to use FR technology. But even this is limited. There are scores of drafted bills that are sitting in legislatures at the municipal, state, or national levels and policy proposals suggested by think tanks that have not yet received a full hearing. Instead, we see many countries taking significant steps to expand their FR infrastructure without any regulation.

We have organized our analysis of FR into five regulatory types. Most common are bans and moratoria, policies mandating consent and notification, and data security policies. A handful of policies and proposals tailor the use of FR, and some organizations have proposed oversight, reporting, and standard-setting policies.

Bans and Moratoria

Bans permanently halt use of FR technology, while moratoria are temporary. Moratoria are usually implemented with the intention of buying time for policymakers and scientists to conduct research and determine the best

way to regulate FR, so that the technology can later be introduced into society in a safe way.

No national-level bans or moratoria have been implemented anywhere in the world. Though the EU developed draft legislation for a 5-year moratorium on FR use in public spaces, it was aborted in February 2020 (Espinoza & Murgia, 2020). However, the United States has implemented multiple bans and moratoria at state and municipal levels.

Bans and moratoria, in practice, typically apply to uses by specific actors, such as law enforcement, commercial entities, in housing, or in employment, rather than encompassing all use of FR technology. Most often, proposals focus on limiting FR use among government agencies and law enforcement. In the United States, the states of New Hampshire and Oregon have banned law enforcement use of FR in body cameras (Crawford, 2019). California recently passed the Body Camera Accountability Act, a statewide three-year moratorium on FR in police body cameras that went into effect on January 1, 2020 (Body Camera Accountability Act, 2019). As noted earlier in this report, in July 2020 the New York state assembly passed a 2-year moratorium on the use of biometric identification technology in schools. It is awaiting the governor's signature. The cities of San Francisco, Berkeley, and Oakland in California as well as Boston, Somerville, Brookline, Northampton, and Cambridge, Massachusetts have banned FR use by government agencies, though it is still legal in private and commercial spaces (Martineau, 2019; Jarmanning, 2020). Portland, Oregon is currently considering a blanket ban on

FR technology, which would include both public and private entities; this proposal is the strictest in the nation (Ellis, 2019). US Senators have proposed bills that would institute a nationwide moratorium on FR use by federal agencies and law enforcement. Senators Cory Booker and Jeff Merkley's Ethical Use of Facial Recognition Act also proposes the creation of a Congressional Commission that would research the technology and recommend guidelines during this time (S. 3284, 2020; Heilweil, 2020b).

Meanwhile, international leaders have issued public calls. At the October 2019 International Conference on Data Protection and Privacy Commissioners in Albania, the Public Voice Coalition, which is composed of more than 100 non-governmental organizations (NGOs) from over 9 countries, called for a global moratorium on mass surveillance through FR (The Public Voice, 2019). Additionally, in June 2019, David Kaye, the United Nations Special Rapporteur on Freedom of Opinion and Expression, called for a moratorium on the sale, transfer, and use of surveillance technology, including FR, until nations could establish regulations to protect human rights standards (Kaye, 2019). Despite this advocacy, there has been no international legal agreement on a FR moratorium.

Finally, there are proposals to prohibit the use of federal funds for implementing or operating FR technology or, similarly, to prohibit use of FR technology in domains that receive federal funds. US Congressional Representative Yvette Clark's No Biometric Barriers to Housing Act would block the use of FR technology in public housing that

gets funds from the Department of Housing and Urban Development (H.R. 4008, 2019). Representative Rashida Tlaib’s H.R. 3875 would prohibit federal funding from being used to purchase or use FR technology altogether (H.R. 3875, 2019).



C-SPAN

Consent and Notification Policies

We found that often governments will group both consent and notification provisions and data security measures together under a single policy. For example, the European Union’s (EU) General Data Protection Regulation (GDPR) and Illinois’s Biometric Information Privacy Act (BIPA) contain both consent and data security protections. However, despite these policies often being grouped together, we view them as having two distinct functions. Data security policies

dictate how to protect data once it is already collected, such as with robust encryption standards or local storage mandates. So, we chose to differentiate between these types of policies as two distinct categories for the purpose of this report.

Meanwhile, consent and notification policies focus on the data collection process, creating requirements about obtaining consent from subjects and notifying individuals about how their data will be used. Data collection entities must notify individuals about how data is collected, where it is stored, what it is used for, when it is used, how it works, and when it is discarded. Another similar policy option focuses on consent: consumers must have the option to opt-out of FR systems, either by never having their data collected, or being able to request deletion of data already collected (often called the “right to be forgotten”). Finally, there are two tiers regarding the extent to which consent must be received for data collection. The stronger option requires that affirmative consent be collected prior to collection of data. A weaker option requires that individuals be notified prior to collection of data, but affirmative consent is not required—consumers must know that their data is being collected, but they may not be empowered to stop it.

One of the most comprehensive policies regulating individuals’ rights to their biometric information is the EU’s General Data Protection Regulation (GDPR). It regulates data protection and privacy in the EU and European Economic Area (EEA), giving individuals control over their personal data and making businesses institute

safeguards to protect data (Voigt & von dem Bussche, 2017). Under the GDPR, businesses must ensure that personal data is collected legally and under highly regulated, controlled conditions. They must clearly disclose to consumers what data is being collected, how long it is being retained, what it is being used for, and with whom it is shared (Tikkinen-Piri et al., 2018). Organizations must either ask that consumers opt-in to data collection or offer an opt-out option. The GDPR also includes the “right to be forgotten”, allowing individuals to request that organizations delete their data (Voigt & von dem Bussche, 2017). The GDPR is significant because it is one of the first major policies to include biometric information under the term “personal information” (Tikkinen-Piri et al., 2018). Japan’s Act on the Protection of Personal Information (APPI) is another example of a nationally implemented consent and notification policy (The Act on the Protection of Personal Information [APPI], 2015). APPI is similar to the GDPR. This law requires that business operators collecting personal information gain consent from and notify subjects about how their data will be used prior to data collection (APPI, 2015).

India has also proposed legislation that emulates the GDPR: the Personal Data Protection Bill of 2019. Introduced in December 2019 by the Minister of Electronics and Information Technology, this bill would provide for the protection of individuals’ personal data and establish a Data Protection Authority (Personal Data Protection Bill, 2019). This bill explicitly includes biometric data. Under this policy, data collection entities would have to obtain consent from individuals whose data they

are collecting, with certain exceptions (Personal Data Protection Bill, 2019). They would also be obligated to implement data security safeguards and grievance redressal mechanisms in case of complaints about data usage (Personal Data Protection Bill, 2019). Finally, citizens would have the right to obtain information from the government and companies about how their data is being used (Personal Data Protection Bill, 2019).

Some US states have adopted similar policies. Illinois’s Biometric Information Privacy Act (BIPA), passed in 2008, requires that proper consent be obtained by businesses when collecting and using biometric information (Insler, 2018). This law allows individuals to sue over the collection and use of their biometric data. The California Consumer Privacy Act, which took effect on January 1, 2020, gives consumers the right to know what personal information is being collected, used, shared or sold, the right to make organizations delete their personal information, the right to opt-out of the sale of personal information, and the right to non-discrimination if they exercise their privacy rights (California Office of the Attorney General, 2019). This policy also requires that businesses provide notice to customers before collecting data.

Though no consent and notification laws regarding biometric technology exist at the federal level in the US, there have been many proposals. Senators Roy Blunt and Brian Schatz proposed the Commercial Facial Recognition Privacy Act to strengthen biometric data protections for consumers by outlawing business collection and use of FR

technology without affirmative consent (S. 847, 2019). Additionally, when the Federal Trade Commission (FTC) issued guidelines for how commercial businesses could best protect consumer privacy in 2012, it specifically outlined that customers should be notified when FR technology is used and have the opportunity to opt out, and they should be given detailed information on how the data is being used and how to delete it (Federal Trade Commission, 2012).

Data Security Policies

As noted above, data security policies aim to safeguard biometric data by requiring encryption and other protections against breach or misuse. In addition to mandating that companies notify and obtain consent from citizens whose data is being collected (consent and notification), the EU's GDPR has provisions that limit the ability of companies to share or sell data with third parties. Japan's APPI and India's proposed Personal Data Protection Bill of 2019 are very similar (APPI, 2015; Personal Data Protection Bill, 2019).

New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, passed in July 2019, requires that businesses implement safeguards to protect the personal information of New York residents and expands the state's security breach notification requirements (Stop Hacks and Improve Electronic Data Security Act [SHIELD], 2019). This law explicitly includes biometric information under its definition of "private information" (SHIELD, 2019). Additionally, the New York State Senate has another data security bill in the assembly

committee. Assembly Bill A1692, if passed, would prohibit state agencies and contractors doing business with state agencies from retaining FR images (A. 1692, 2020).



Blogtrepneur

Think tanks and policy research organizations have offered multiple data security proposals. The US Brookings Institution, for example, has recommended that FR data only be stored for a limited time, after which it must be destroyed (West, 2019). The length of storage time would depend on the relative sensitivity and purpose of the data. Brookings also recommends policies that restrict data sharing by limiting the ability of companies to transmit, share, or sell data to other companies (as is codified in the GDPR) and that companies reduce collateral information collection: that is, organizations should collect the minimum amount of data necessary to complete the given task (West, 2019).

The Heritage Foundation, also based in the United States, recommends that biometric

systems be designed for local data storage (data is stored on the device that collected it) rather than in a centralized data hub (data is sent from the collecting apparatus to centralized storage; for example, in a cloud) (Rosenzweig et al., 2004). Centralized storage is less private and more prone to breach. The Brookings Institution has also made this recommendation (West, 2019). Some companies that sell FR products have heeded this recommendation; most famously, Apple stores the data that powers its Face ID iPhone function locally on each user's phone—this data is never uploaded to a cloud (Apple, 2020). The Heritage Foundation also recommends that biometric systems reduce data to a template rather than storing the image itself. Templates are harder to falsify and therefore more secure, reducing the likelihood of consumers' sensitive biometric information being stolen (Rosenzweig et al., 2004).

Some propose minimum standards for strength of data protection, including certain standards for data encryption or anonymization. Senators Roy Blunt and Brian Schatz's Commercial Facial Recognition Privacy Act proposes: "The bill...would require facial recognition providers to meet data security, minimization, and retention standards as determined by the Federal Trade Commission and the National Institute of Standards and Technology" (S. 847, 2019).

Policies to Tailor Use

Some policies and policy proposals attempt to specify acceptable uses of the technology. Detroit, Michigan's Project Green Light

program, for example, is a law enforcement video surveillance system with hundreds of cameras located at private businesses and intersections that transmit real-time footage with FR capabilities to the police department (Harmon, 2019). This program sparked massive public opposition, due to concern that it could widen the net of criminalizing and targeting vulnerable Detroiters. In September 2019, the Detroit Board of Police Commissioners responded by banning live-stream use of FR; the technology can now only be used when analyzing footage after the fact. The Board also restricted use to investigations of violent crimes or home invasions (Gross & Jones, 2019). Finally, the city banned the use of FR technology for immigration enforcement (Gross & Jones, 2019). In this way, Detroit codified in policy acceptable uses of the technology.

Sweden's Data Protection Authority (DPA) recently concluded that law enforcement use of FR was permissible. In 2019, Swedish police submitted to the DPA an impact assessment on their use of FR technology for approval, as there had previously been no explicit guidance on its legality. The DPA concluded that police's privacy and storage measures were in compliance with Sweden's Crime Data Act and the EU's Data Protection Law Enforcement Directive, and therefore their use of this technology was permissible on a national scale (Hoy, 2019). The DPA also concluded that FR would help police do their jobs more effectively (Hoy, 2019). Senators Chris Coons and Mike Lee have proposed a similar policy at the US federal level: the Facial Recognition Technology Warrant Act (S. 2878, 2019). It would require federal agencies to get a warrant before using

FR technology when conducting targeted, ongoing surveillance on the public.

Oversight, Reporting, and Standard-Setting Policies

Oversight, reporting, and standard-setting regulations mandate different ways of observing and controlling the operations of FR systems, including their accuracy. These types of policies have been widely proposed but not yet implemented.

The Brookings Institution suggests requiring third-party testing of FR technologies prior to implementation and periodically throughout use (West, 2019). This testing would aim to ensure accuracy, lack of bias, high data security and, in the United States, compliance with Federal Trade Commission (FTC) and NIST rules. The proposed Commercial Facial Recognition Privacy Act of 2019, which is currently stalled in the US Congress, would require third-party testing of FR systems prior to implementation (S. 847, 2019).

The Brookings Institutions also recommends strict accuracy standards for FR systems, which would be determined by NIST or another regulatory body. For example, legislation could set a mandatory threshold accuracy requirement, such as 95% of faces identified accurately, for the system to be eligible for implementation. Brookings also argues that the accuracy standards for FR should be proportional to the gravity of its use: for example, law enforcement should have the highest accuracy standards, because

the consequences of falsely identifying a suspect could cause irreparable damage (West, 2019). In November 2019, China established a national working group of 28 technology companies to set standards for FR related to both technology and ethics, called the National Standardization Group for Facial Recognition Technology (Yan, 2019). Though these standards have not been finalized or released, this is still an example of prioritizing standard-setting.

Another approach focuses on reporting requirements for entities who use FR. This would require those who use these systems to disclose how they are used and their impacts, which could aid future development of the technology and help regulators police problems. Such a policy was passed in Congress as an amendment in July 2019: H. Amdt. 577 to H.R. 3494, the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020. This amendment required the Director of National Intelligence to submit a report to Congress about the intelligence community's use of FR technology. This amendment also required that this report clearly acknowledge that using FR technology to suppress dissent is unethical, and that the US government should not sell FR technology to any country that uses it to suppress human rights (H. Amdt. 577, 2019). In this way, the policy tool of setting reporting requirements can be used not only to gather information but also to influence the ethics and ideals behind the use of FR technology.

Facial Recognition Expansion Without Regulation

Meanwhile, many nations are actively instituting FR systems without regulation. For example, Mexico City has recently invested \$10 million in installing thousands of FR-enabled security kits that monitor the public in 56 communities across the city (Government of Mexico City, 2019). Additionally, in Ecuador's capital Quito, 78 FR cameras were installed in late 2019, forming a new citywide biometric surveillance system (Bravo, 2019). Serbia's capital of Belgrade also recently instituted a major citywide FR surveillance system (CBS News, 2019). Belgrade's surveillance system was created by Huawei, the Chinese telecommunications company, and aims to eventually institute 1,000 cameras in 800 locations in Belgrade (CBS News, 2019). Huawei's system, called Safe Cities, has been instituted in 230 cities across Turkey, Russia, Ukraine, Kenya, Uganda, Germany, France, and Italy—to name a few (CBS News, 2019). We have found no explicit information indicating any regulation of or intention to regulate FR in these nations.

In the European Union, which is subject to the GDPR, individual countries are experimenting with how they can use FR, while remaining in compliance with the GDPR. For example, the German interior ministry launched a small-scale FR trial in the Berlin Südkreuz railway station, in order to test the accuracy and popularity of such a system (Delcker, 2018). In 2017, the ministry recruited 300 volunteers

who frequently traveled through the station, who agreed to submit biometric photos to a database and carry a transponder with them (Delcker, 2018). The project sparked



David Iliff, CC BY-SA 3.0

massive public opposition as it was criticized for lacking transparency and threatening privacy (Delcker, 2018). Additionally, in recent months, Sweden has grappled with what uses of FR are and are not permissible under the GDPR. As detailed above, Sweden has explicitly allowed law enforcement to utilize FR, but has also condemned the use of FR in schools as we describe further below (Hoy, 2019; BBC News, 2019b). Both of these decisions were made by Sweden's Data Protection Authority, which monitors and enforces GDPR compliance (Hoy, 2019; BBC News, 2019b). This demonstrates how nations subject to FR policies experiment with the extent to which they can implement FR systems in a piecemeal approach.

Regulating Facial Recognition in Schools

There are currently no policies anywhere in the world that explicitly regulate the use of FR technology in schools. However, there has been debate over the use of FR in the educational space in many countries. In September 2019, the Chinese government's Ministry of Education announced that it intended to "curb and regulate" the use of FR and similar technology in schools, and recommended that any schools thinking of installing the technology seek the opinions of students, teachers, and parents before doing so (BBC News, 2019a). They cited data security and privacy issues (Jin, 2019). Since then, eight federal departments, including the Ministry of Education, jointly issued the "Opinions on Guiding the Orderly and Healthy Development of Educational Mobile Internet Applications". This document made recommendations about how technology should be used in education, including asking administrators to notify and gain consent from subjects regarding the purposes and methods of data collection and recommending the collection of minimal amounts of data, as well as other privacy and data security measures (Jin, 2019). Despite this progress on the issue, there has not yet been any actual legislation in China regulating FR in schools.

Both the French and Swedish governments have determined that this use is not permissible under the GDPR. The French advocacy group for digital rights and freedoms, La Quadrature du Net, filed

lawsuits against high schools in Nice and Marseille that were piloting FR systems (Kayali, 2019). The Administrative Court of Marseille found that installation of this technology in schools violated the GDPR's privacy regulations, because students could not freely consent to this system (Kayali, 2019). This technology also violated the GDPR's principles of proportionality and data minimization. Additionally, Sweden's DPA fined the Skelleftea municipality for piloting a FR trial in local high schools that tracked student attendance (BBC News, 2019b). The DPA argued that high schools could achieve the same ends in a less intrusive way, as required by the GDPR. Hence, though no laws have been passed specifically regulating FR in schools in Europe, courts and regulatory bodies have already determined that the GDPR applies in school settings, thus setting a precedent that FR use in schools should be prohibited.



Kyle S. Mackie / WBFO News

In the United States, New York Senate Bill S. 5140B, if passed, would prohibit the use of biometric technology in all New York schools

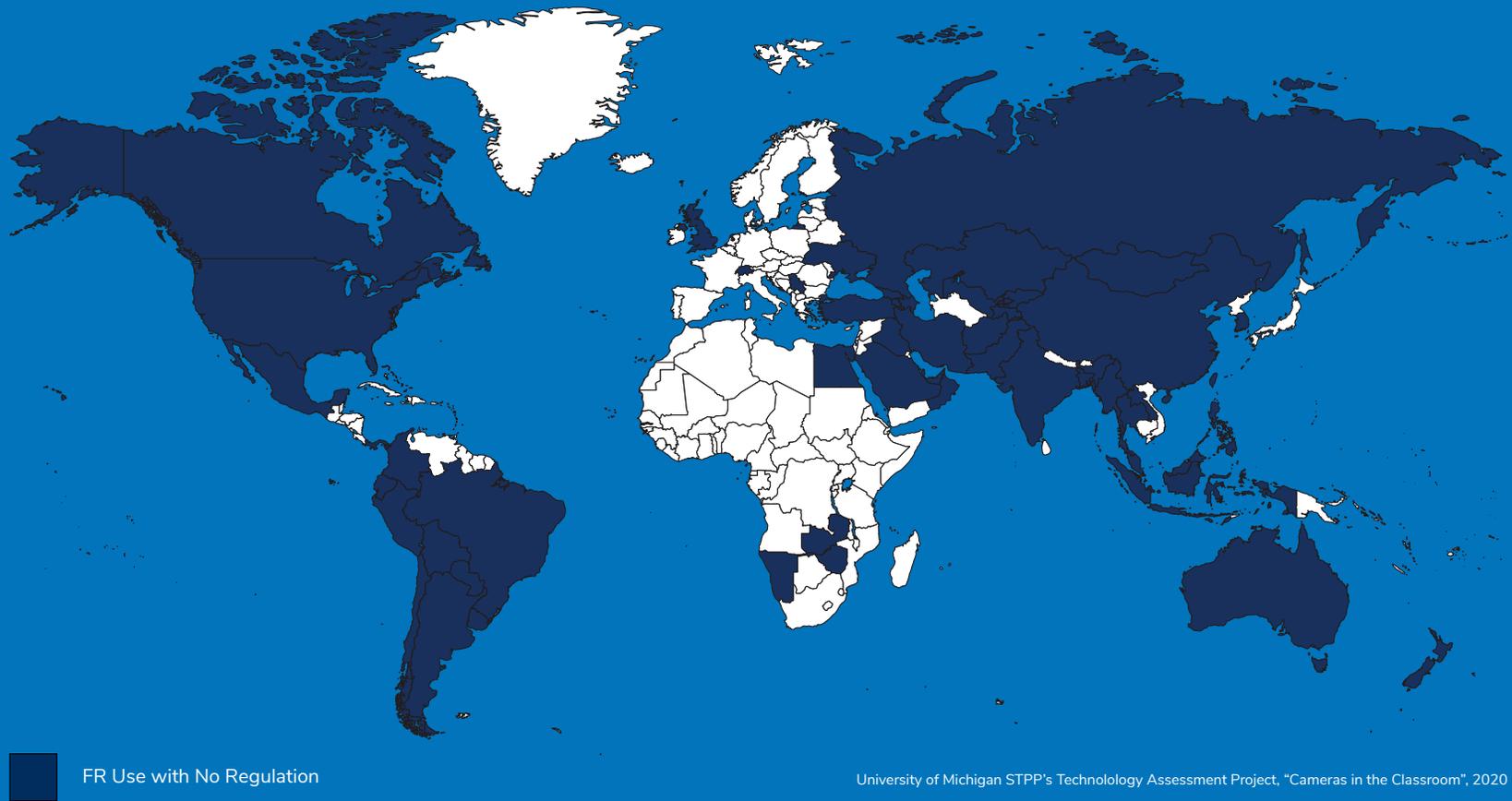
until July 2022. This bill would direct the Commissioner of Education to conduct a study on the reliability, privacy implications, security implications, bias, risk to data security, and expected cost of biometric technology in schools during this time, and ultimately submit a recommendation for future legislation (New York Civil Liberties Union, n.d.). This bill is supported by the New York Civil Liberties Union. As of July 22, 2020, it was passed by both the New York State Assembly and Senate, meaning that it now only needs Governor Cuomo's signature for passage.

While S. 5140B is the only proposal that specifically regulates FR use in schools in the United States, other policies are relevant to this practice in the US. The Family Educational Rights and Privacy Act (FERPA) prohibits the sharing of certain information

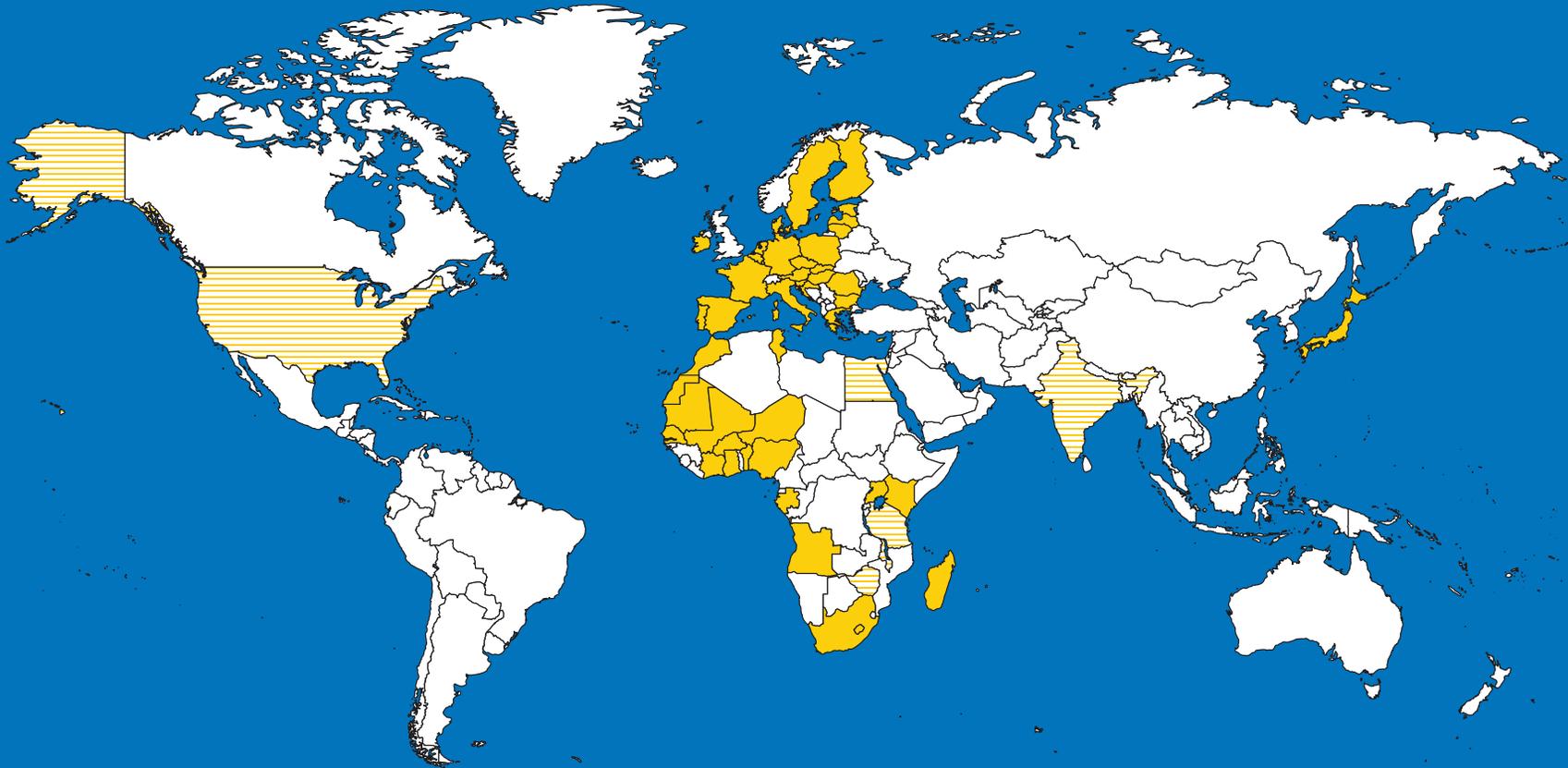
(including biometric data) in educational records without consent (US Department of Education, 2018). It also gives parents and guardians some control over the disclosure of personally identifiable information from these records, requiring parental consent if they want to disclose certain types of student information (US Department of Education, 2018). And, the Children's Online Privacy Protection Act (COPPA) protects the privacy of children under 13 years old by requiring parental consent for collection and use of children's personal information. This act requires full disclosure to parents and guardians of any information collected from children, and the right to invoke consent and have information deleted (Electronic Privacy Information Center, n.d.).

National and International Policy Maps

Map A: Countries Using Facial Recognition without National Regulation



Map B: Facial Recognition Policies at the National Level



-  No Policy
-  Only Proposed Policies
-  Passed Policies

Sources for Map Data

In order to understand the full extent of FR use and policies in each country and US state, we did our own searches across a variety of sources. (There is no single comprehensive report covering this.) To inform Map A: Countries Using Facial Recognition without National Regulation, we used the Carnegie Endowment for International Peace’s AI Global Surveillance (AIGS) Index (Feldstein, 2019). This index indicated each national government that uses FR. We then removed the countries that had regulatory policies in place. For Map B: Facial Recognition Policy Status by Country two of us, working

independently, searched Google repeatedly using a variety of search terms. We also used Deloitte’s report “Privacy is Paramount: Personal Data Protection in Africa”. We included every European Union nation since they all fall under the GDPR. Finally, for Map C: Facial Recognition Policy Status by US States, we gathered data primarily from resources created by Fight for the Future, the Electronic Privacy Information Center, Wired, and the Project on Government Oversight, in addition to Google (Fight for the Future, n.d.; Electronic Privacy Information Center, n.d.; Crawford, 2019; Ulle, 2019). For access to the raw data that informed these maps, email stpp@umich.edu

Our Facial Recognition Future

Analyzing all of the analogical case studies and themes above, a story begins to emerge about the likely outcomes of widespread FR adoption in K-12 schools. The five types of implications we identified suggest that rather than reducing the frequency of school shootings or school violence, FR in schools will further exacerbate racial inequality in education, erode students' privacy, punish individuality, produce new markets for companies to profit from childrens' biometric data, and struggle with accuracy.

The history of "school safety" technologies like metal detectors and school resource officers tells us that FR systems will disproportionately target Black and brown students. Because FR systems are less accurate with non-white faces, students of color are more likely to trigger false positives in the system, exposing them to additional security measures, and over time decreasing their sense of safety, trust, and belonging in school. False positives will also increase the interactions between Black and brown children and school police or security officers, which increases the risk of violence, arrest, and suspension. Finally, because FR systems are not free of human biases and yet are often assumed to be objective, FR in schools is poised to disproportionately target minorities, just as the stop and frisk policing policy did. This will result in the

legitimization, institutionalization, and weaponization of racial biases against Black and brown students.

Children today are already experiencing much greater levels of surveillance than anything their parents experienced. We saw with CCTV systems that these erosions of privacy have real consequences. Rather than simply identifying potential intruders, FR systems are likely to become tools for monitoring student behavior and enforcing compliance. When students believe they are always being watched, they feel powerless and mistrusted. Some will change their behavior in order to



avoid scrutiny, while others who are unable to fit into the narrowed definition of acceptable behavior, such as students of color, trans and gender non-conforming students, and students with disabilities, will be further marginalized and alienated.

Technology companies have become increasingly adept at commodifying all kinds of data, including biometric data like blood spots and fingerprints, and then combining this with publicly identifiable data. The same is already true for FR, and deploying FR systems in schools will mean putting children's faces into those markets. FR data may generate more revenue than sales of the systems themselves, and without clear regulation around consent and retention, companies will be free to use and profit from their collection of student facial data with no recourse for the children and families whose lives have been adversely affected by FR. Furthermore, failures to sufficiently safeguard FR data produce the very real risk that hacks or breaches will have long-lasting effects, following students throughout their lives.

Accuracy will be a persistent problem. As with breathalyzer systems, most FR implementation in schools will not have adequate staffing or training to maintain reliable accuracy. Due to limited regulation and wide variation in commercial products, it will be difficult for administrators to assess the accuracy of their systems and their effectiveness in preventing low probability events such as school shootings. Once schools expend the money to install FR, the systems will become entrenched, regardless of adverse outcomes or ineffectiveness. Finally, FR is often marketed as a way to increase efficiency and reduce costs, which may result in cuts to security staffing, and therefore no human on site to deal with false positives or other system failings.

With the possibility of this future in mind, it is difficult to imagine a scenario in which the benefits of FR in schools outweighs the risks. Below we offer recommendations for policymaking at the national, state, and local level that are informed by this analysis.

Recommendations

Given the legacies of the technologies we have reviewed throughout this report, we find it difficult to imagine that the benefits of FR technology will outweigh the risks. Rather, we conclude the opposite: at the time of a technology's introduction, we tend to overestimate the benefits and minimize the negative consequences. Therefore, 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. This approach is necessary in order to ensure societal benefit and public legitimacy for FR.

In what follows, we provide recommendations to both national and local policymakers, on how they might proceed if they feel it is absolutely necessary to implement the technology.



We strongly recommend that FR technology be banned for use in schools.

What can individual schools, parents/guardians, and students do?

In **Appendices A** and **B** of this report, we offer questions you can ask policymakers and FR providers, to help you evaluate the technology and its proposed use, and advocate for a ban or regulation.

Below we provide policy recommendations if schools decide it is absolutely necessary to implement the technology.

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. The EU's GDPR is a good model for a law that protects sensitive personal information and gives consumers control over their data. This would shape the development and use of a variety of digital technologies, not just FR.

However, instituting nationwide data privacy and security laws is just the first step for regulating FR. Because the issues raised by FR go far beyond data privacy and security, FR requires its own regulatory attention and framework.

3

Convene a **national advisory committee** to investigate FR and its expected implications, and **to recommend a regulatory framework** to govern this technology. The framework should require that FR companies meet high standards for the following criteria: transparency regarding the technical development of FR, including the algorithms used, the data on which the algorithm is trained (and how it is updated), and error rates; accuracy (for false positives and negatives); disparate impacts, i.e., whether and how the technology might disproportionately hurt vulnerable populations, including people of color, gender non-conforming students, and the disabled; data management practices, including storage, access, collection, and cybersecurity; and clear requirements for ongoing maintenance, that are feasible for schools.

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 in charge of or attending kindergarten through high school (K-12) schools operations, including teachers, school administrators, superintendents, high school students, and parents and guardians of elementary and middle school students. Government officials from relevant agencies (e.g., Department of Education, 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** (Gutmann and Thompson, 2004).

4

Create additional oversight mechanisms for the technical dimensions of FR. A federal agency should set accuracy thresholds (a certain level of false positives or negatives at which the FR system is designated unusable), reporting requirements for users, and infrastructure for regularly and systematically evaluating and overseeing FR systems. In the United States, for example, the National Institute for Standards and Technology could increase its current oversight to include these dimensions.

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. The state-level committee should include the same types of expertise as the national level, and cover the same issues: it should provide guidance to school districts, schools, teachers, parents, and students on how to evaluate FR technologies before purchase and the expertise and resources needed at the local level to deploy these technologies safely.

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. Schools should consider the full range of costs and benefits over the lifetime of the technology when making this determination, including effects on student and parent behavior and cost. Schools should engage a FR advisory committee (with similar demographic and intellectual diversity as the one recommended for the national level) during this stage.

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. The evaluation should consider the transparency of both the data and algorithm behind the FR technology, accuracy of face-matching (including among Black, brown, gender non-conforming, and disabled people), methods of alleviating any bias in the technology and ensuring equity, and data management practices. Evaluation criteria should be developed using an advisory committee with the types of expertise outlined above.

9

Develop a plan for implementing the technology before using it. As with the evaluation plan, this is particularly important if there is no national or state-level guidance on the issue. The plan must include rules and procedures regarding disparate impacts, data management, maintenance and ensuring accuracy, grievance and appeals procedures, and communication with teachers, parents, guardians, and students. It should be developed using an advisory committee with the types of expertise outlined above.

10

Do not purchase FR systems that use student social media accounts to improve the technology. During the evaluation process, schools should ask whether the company uses student social media to create image databases, and should not contract with any company that does this unless the feature can be permanently disabled.

11

Do not use FR technology to police student behavior. If schools use it in this way they must have much higher accuracy thresholds than for other uses, including identifying visitors to campus. There should also be an easily accessible grievance and appeals procedure for students, parents, and guardians before the technology is used for this purpose.

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. This technically-trained person would ensure that the system is working properly at all times, that it is being used for its intended purposes, and that the system is operating in accordance with all relevant laws. They would be familiar with existing school policy, school security operations, and should have sufficient technical expertise to communicate with the FR company and manage relevant hardware and software. A school district with multiple schools using FR should also have at least one person providing oversight.

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. Before the pilot period begins, school administrators should decide on the criteria for a successful program. Criteria should include: whether there has been greater safety on campus, whether crime has shifted off campus, how many false matches resulted, whether appeals received due process, social and psychological impact on students and families, how frequently the system was maintained and whether this was adequate, whether expertise and training of staff to maintain the technology has been adequate, and the costs of maintenance. Before the pilot period begins, schools should collect relevant data on its operations. This will allow the school to gauge the impacts of the technology at the end of pilot period.

If, after the pilot period, the FR system is not successful along these criteria, it should be removed, or the school should significantly alter how it is used. If it chooses to alter use, it should then initiate another pilot period prior to full-scale implementation. FR companies must accommodate this pilot period; that is, the first contract should only extend through the pilot period and should be re-negotiated if the school decides to implement FR for the longer term.

Acknowledgements

The authors would like to thank Rebecca Ackerman, Ben Green, Justin Joque, Catherine Morse, Nick Pfof, Joy Rohde, and Nicole Scholtz for their assistance in researching, revising, and producing this report.



References

- Acquisti, A., Gross, R., & Stutzman, F. D. (2014). Face recognition and privacy in the age of augmented reality. *Journal of Privacy and Confidentiality*, 6(2). <https://doi.org/10.29012/jpc.v6i2.638>
- Advancement Project. (2018). *We came to learn: A call to action for police free schools*. <https://advancementproject.org/wecametolearn/>
- Ahmed, M. (2018, May 11). *Aided by Palantir, the LAPD uses predictive policing to monitor specific people and neighborhoods*. *The Intercept*. <https://theintercept.com/2018/05/11/predictive-policing-surveillance-los-angeles/>
- Alabama Appleseed Center for Law and Justice. (2019). *Hall monitors with handcuffs: How Alabama's unregulated, unmonitored School Resource Officer Program threatens the state's most vulnerable children*. <https://www.alabamaappleseed.org/wp-content/uploads/2019/08/Alabama-Appleseed-Hall-Monitors-with-Handcuffs.pdf>.
- Alba, D. (2020, February 6). Facial recognition moves into a new front: Schools. *The New York Times*. <https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html>
- Amazon Web Service. (n.d.). *The facts on facial recognition with artificial intelligence*. <https://aws.amazon.com/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/>
- American Civil Liberties Union. (2017). *Bullies in blue: The origins and consequences of school policing*. <https://www.aclu.org/report/bullies-blue-origins-and-consequences-school-policing>
- Anderson, K. (2001, August 20). *Anger over face-scanning cameras*. *BBC News*. <http://news.bbc.co.uk/2/hi/science/nature/1500017.stm>
- A. 1692, 2019–2020 New York State Senate, 2019–2020 Leg. Session. (NY. 2020).
- Apple. (2020, February 26). *About Face ID advanced technology*. <https://support.apple.com/en-us/HT208108>
- Arudpragasam, A. (2018, March 23). *Aadhaar: The potential and limitations of India's Digital ID*. *Harvard Kennedy School Ash Center*. <https://www.innovations.harvard.edu/blog/aadhaar-potential-and-limitations-india-s-digital-id>
- Bergh, A. K., Lucas, D. M., Hallett, R. A., Huber, R. A., Fennell, E. J., Coldwell, B. B., Hoday, J., Ackland, K., Picton, W. R. (2013). *Recommendations of the Canadian Society of*

- Forensic Science on breath testing standards & procedures. *Canadian Society of Forensic Science Journal*, 2(4), 88–93. <https://doi.org/10.1080/00085030.1969.10757077>
- Birnhack, M., Perry-Hazan, L., & Ben-Hayun, S. G. (2017). CCTV surveillance in primary schools: Normalisation, resistance, and children's privacy consciousness. *Oxford Review of Education*, 44(2), 204–220. <https://doi.org/10.1080/03054985.2017.1386546>
- Bijker, W.E., Hughes, T.P. and Pinch, T. eds. (1987). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press.
- Bohannon, J. (2015, January). Unmasked. *Science*, 347(6221), 492–494.
- Bravo, D. (2019, December 9). 78 cámaras de reconocimiento facial fueron instaladas en el Centro Histórico de Quito; 13 de ellas solo en La Marín. *El Comercio*. <https://www.elcomercio.com/actualidad/camaras-reconocimiento-facial-quito-marin.html>
- Brayne, S. (2014). Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review*, 79(3), 367–391. <https://doi.org/10.1177/0003122414530398>
- Brennan, D. S. (2017, April 26). Vista district using fingerprint scans for school lunches. *The San Diego Union-Tribune*. <https://www.sandiegouniontribune.com/communities/north-county/sd-no-vista-fingerprinting-20170426-story.html>
- Bridges, R. v The Chief Constable of South Wales Police, EWHC 2341 (2019).
- Bridgman, A. (1983). *Missing-children phenomena fuels school-fingerprinting programs*. Education Week. <https://www.edweek.org/ew/articles/1983/10/19/04070027.h03.html>
- Bronskill, J. (2012). Flying the secret skies: difficulties in obtaining data on Canadian airport security screening tests following 9/11. In K. Walby (Ed.), *Brokering access: Power, politics, and freedom of information process in Canada* (pp. 97–114). Vancouver, Canada: University of British Columbia Press.
- Brown, B. (2006). Understanding and assessing school police officers: A conceptual and methodological comment. *Journal of Criminal Justice*, 34(6), 591–604. <https://doi.org/10.1016/j.jcrimjus.2006.09.013>
- Browne, S. (2015). *Dark matters: On the surveillance of Blackness*. Duke University Press Books.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1–15.
- Burton, W. (2019, July 5). Opinion: It's time for a public referendum on Detroit's Project Green Light facial-recognition surveillance technology. *Detroit Metro Times*. <https://www.metrotimes.com/news-hits/archives/2019/07/05/opinion-its-time-for-a-public-referendum-on-detroits-project-green-light-facial->

recognition-surveillance-technology

California Office of the Attorney General. (2019). *California Consumer Privacy Act (CCPA): Fact sheet*. https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

California's Body Camera Accountability Act, Cal. Assemb. 1215 (2019-2020), Chapter 579

Center for Constitutional Rights. (2012). *Stop and frisk: The human impact*. <https://ccrjustice.org/stop-and-frisk-human-impact>

Chan, T. F. (2018, May 20). *A school in China is monitoring students with facial-recognition technology that scans the classroom every 30 seconds*. Business Insider. <https://www.businessinsider.com/china-school-facial-recognition-technology-2018-5>

China to curb facial recognition and apps in schools. (2019a, September 6). BBC News. <https://www.bbc.com/news/world-asia-49608459>

Chinese facial recognition tech installed in nations vulnerable to abuse. (2019, October 16). CBS News. <https://www.cbsnews.com/news/china-huawei-face-recognition-cameras-serbia-other-countries-questionable-human-rights-2019-10-16/>

Ciuriak, D. (2018). *The economics of data: Implications for the data-driven economy*. Chapter 2 in "Data governance in the digital age". Centre for International

Governance Innovation. <https://ssrn.com/abstract=3118022>

Cole, S. (2003). Fingerprinting: The first junk science. *Oklahoma City University Law Review*, 28(1), 73-92.

Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019)

Cope, N. (2004). Intelligence led policing or policing led intelligence? Integrating volume crime analysis into policing. *The British Journal of Criminology*, 44(2), 188-203. <https://doi-org/10.1093/bjc/44.2.188>

Cope, S., Kalia, A., Schoen, S., & Schwartz, A. (2017). *Digital privacy at the US border: Protecting the data on your devices*. Electronic Frontier Foundation. <https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf>

Cornell Law School. (2019, December). *Stop and frisk*. https://www.law.cornell.edu/wex/stop_and_frisk

Cowley, S., & Silver-Greenberg, J. (2019, November 3). These machines can put you in jail. Don't trust them. *The New York Times*. <https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html>

Craven, J. (2016). *Baltimore schools cops' abuse of kids is rooted in city's racist history*. Huffington Post. https://www.huffpost.com/entry/baltimore-school-police_n_57b227f7e4b007c36e4fcb44

- Crawford, S. (2019, December 16). *Facial recognition laws are (literally) all over the map*. *Wired*. <https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/>
- Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993)
- Dee, T. S., & Murphy, M. (2019). Vanished classmates: The effects of local immigration enforcement on school enrollment. *American Educational Research Journal*, 57(2), 694-727. <https://doi-org.proxy.lib.umich.edu/10.3102/0002831219860816>
- Delcker, J. (2018, September 13). Big Brother in Berlin. *Politico*. <https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/>
- Deloitte. (2017). *Privacy is paramount: Personal data protection in Africa*. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf
- Denny, J. C., Rutter, J. L., Goldstein, D. B., Philippakis, A., Smoller, J. W., Jenkins, G., & Dishman, E. (2019). The “All of Us” research program. *The New England Journal of Medicine*, 381, 668-676.
- Doshi, V. (2018, January 4). A security breach in India has left a billion people at risk of identity theft. *The Washington Post*.
- Dror, I., Charlton, D., & Peron, A. (2006). Contextual information renders experts vulnerable to making erroneous identifications. *Forensic Science International*, 156(1), 74-8. <https://doi.org/10.1016/j.forsciint.2005.10.017>
- Electronic Privacy Information Center. (n.d.). Children’s Online Privacy Protection Act (COPPA). <https://epic.org/privacy/kids/>
- Electronic Privacy Information Center. (n.d.). *State facial recognition policy*. <https://epic.org/state-policy/facialrecognition/>
- Ellis, R. (2019, September 17). *Portland considers banning use of facial recognition software in private sector*. Oregon Public Broadcasting. <https://www.opb.org/news/article/portland-facial-recognition-software-private-sector-use-ban/>
- Elsaesser, C., Gorman-Smith, D., & Henry, D. (2013). The role of the school environment in relational aggression and victimization. *Journal of Youth and Adolescence*, 42(235). <https://doi.org/10.1007/s10964-012-9839-7>
- Elvy, S. (2018). Commodifying consumer data in the era of the internet of things. *Boston College Law Review*, 59(2), 423-522.
- Ensign, D., Friedler, S., Neville, S., Scheidegger, C., & Venkatasubramanian, S. (2018). Runaway feedback loops in predictive policing. *Proceedings of Machine Learning Research*, 81, 1-12.
- Espinoza, J., & Murgia, M. (2020, February 11). EU backs away from call for blanket ban on facial recognition tech. *The Financial*

Times. <https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5>

Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020)

Facial recognition: School ID checks lead to GDPR fine. (2019b, August 27). BBC News. <https://www.bbc.com/news/technology-49489154>

Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019)

Federal Trade Commission. (2012, October 22). *FTC recommends best practices for companies that use facial recognition technologies*. <https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition>

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>

Feng, E. (2019, December 16). *How China is using facial recognition technology*. NPR. <https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology>

Ferguson, A. (2011). Crime mapping and the fourth amendment: Redrawing 'High Crime Areas.' *Hastings Law Journal*, 63(1), 179–232. <https://ssrn.com/abstract=1774876>

Ferguson, A. (2016). Policing predictive policing. *Washington University Law Review*, 94(5), 1115–1194. <https://ssrn.com/abstract=2765525>

Ferguson, A. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York, NY: NYU Press.

Ferraraccio, M. (1999). Metal detectors in the public schools: Fourth amendment concerns. *Journal of Law & Education*, 28(2), 209–229.

Fight for the Future. (n.d.). *Ban facial recognition map*. <https://www.banfacialrecognition.com/map/>

Fisher, B. W., Gardella, J. H., & Tanner-Smith, E. E. (2019). Social control in schools: The relationships between school security measures and informal social control mechanisms. *Journal of School Violence*, 18(3), 347–361. <https://doi.org/10.1080/15388220.2018.1503964>

Fisher, E., Mahajan, R. L., & Mitcham, C. (2006). Midstream modulation of technology: Governance from within. *Bulletin of Science, Technology & Society*, 26(2), 485–496. <https://doi.org/10.1177/0270467606295402>

Food and Drug Administration. (2020). *Product Code Classification Database*. <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfPCD/classification.cfm?ID=DJZ>

Fussey, P. (2007). Observing potentiality in the global city: Surveillance and counterterrorism in London. *International*

- Criminal Justice Review*, 17(3), 171–192.
<https://doi.org/10.1177/1057567707306577>
- Garcia, M., & Castro, S. (2011). *Blowout!: Sal Castro and the Chicano struggle for educational justice*. Chapel Hill, NC: University of North Carolina Press.
- Gastic, B. (2011). Metal detectors and feeling safe at school. *Education and Urban Society*, 43(4), 486–498. <http://dx.doi.org/10.1177/0013124510380717>
- Gastic, B., & Johnson, D. (2015). Disproportionality in daily metal detector student searches in US public schools. *Journal of School Violence*, 14(3), 299–315.
- Gates, K. (2011). *Our biometric future: facial recognition technology and the culture of surveillance*. New York: NYU Press.
- Gelman, A., Fagan, J., & Kiss, A. (2007). An analysis of the New York City Police Department’s “Stop-and-Frisk” policy in the context of claims of racial bias. *Journal of the American Statistical Association*, 102(479), 813–823.
- Goel, V. (2018, April 7). ‘Big Brother’ in India requires fingerprint scans for food, phones and finances. *The New York Times*. <https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html>
- Goldstein, M. (2017). *TSA misses 70% of fake weapons but that’s an improvement*. Forbes. <https://www.forbes.com/sites/michaelgoldstein/2017/11/09/tsa-misses-70-of-fake-weapons-but-thats-an-improvement/#7185662e2a38>
- Gorner, J., & Sweeney A. (2020, January 24). For years Chicago Police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended. *Chicago Tribune*. www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html.
- Government of Mexico City. (2019). *Visión 360*. <https://www.jefaturadegobierno.cdmx.gob.mx/storage/app/media/pdf-vision-360-vf.pdf>
- Gotwalt, E. (1992). Case comment: Moore v. Regents of University of California. *Food and Drug Law Journal*, 47(2), 225–245.
- Gray, S. (2007, September 25). *Should schools fingerprint your kids?* Time. <http://content.time.com/time/business/article/0,8599,1665119,00.html>
- Greene, J. (2020, June 11). Microsoft won’t sell police its facial-recognition technology, following similar moves by Amazon and IBM. *The Washington Post*. <https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/>
- Greenfield, D. L. (2006). Greenberg v. Miami Children’s Hospital: Unjust enrichment and the patenting of human genetic material. *Annals of Health Law*, 15, 213–249.

- Griffiths, J. (2019, December 2). *China is rolling out facial recognition for all new mobile phone numbers*. CNN. <https://www.cnn.com/2019/12/02/tech/china-facial-recognition-mobile-intl-hnk-scli/index.html>
- Gross, A., & Jones, R. (2019, September 20). *New rules over facial recognition approved, but distrust and confusion remain*. WXYZ Detroit. <https://www.wxyz.com/news/local-news/investigations/new-rules-over-facial-recognition-approved-but-distrust-and-confusion-remain>
- Grossman, L. (2001, February 4). *Welcome to the Snooper Bowl*. Time. <http://content.time.com/time/magazine/article/0,9171,98003,00.html>
- Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (FRVT) part 3: demographic effects*. Department of Commerce. <https://doi.org/10.6028/NIST.IR.8280>
- Guston, D. H., & Sarewitz, D. (2002). Real-time technology assessment. *Technology in Society*, 24(1-2), 93-109. [https://doi.org/10.1016/S0160-791X\(01\)00047-1](https://doi.org/10.1016/S0160-791X(01)00047-1)
- Gutmann, A., & Thompson D. (2004). *Why deliberative democracy?* Princeton, NJ: Princeton University Press.
- Hacker, K., Chu, J., Leung, C., Marra, R., Pirie, A., Brahimi, M., English, M., Beckmann, J., Acevedo-Garcia, D., & Marlin, R. P. (2011). The impact of Immigration and Customs Enforcement on immigrant health: Perceptions of immigrants in Everett, Massachusetts, USA. *Social Science & Medicine*, 73(4), 586-594.
- H. Amdt. 577, Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, H.R. 3494, 116th Cong. (2019).
- Hamlett, P., Cobb, M. D., & Guston, D. H. (2013). National citizens' technology forum: Nanotechnologies and human enhancement. *Nanotechnology, the Brain, and the Future*, 265-283. https://doi.org/10.1007/978-94-007-1787-9_16
- Han, H., & Jain, A. (2014). Age, gender and race estimation from unconstrained face images. *Technical report MSU-CSE-14-5*.
- Hankin, A., Hertz, M., & Simon, T. (2011). Impacts of metal detector use in schools: Insights from 15 years of research. *Journal of School Health*, 81(2), 100-106.
- Harmon, A. (2019, July 8). As cameras track Detroit's residents, a debate ensues over racial bias. *The New York Times*. <https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html>
- Harwell, D. (2019a, April 30). Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong? *The Washington Post*. <https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/>

Harwell, D. (2019b, December 19). Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. *The Washington Post*. <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>

Haskins, P. (2019). *Research will shape the future of proactive policing*. National Institute of Justice Journal. <https://nij.ojp.gov/topics/articles/research-will-shape-future-proactive-policing>

Heilweil, R. (2020a, January 14). *Why activists want to ban facial recognition on college campuses before it arrives*. Vox. <https://www.vox.com/recode/2020/1/14/21063689/facial-recognition-college-campuses-universities-fight-for-the-future>

Heilweil, R. (2020b, February 19). *How a basic iPhone feature scared a senator into proposing a facial recognition moratorium*. Vox. <https://www.vox.com/recode/2020/2/19/21140503/facial-recognition-jeff-merkley-regulation-clearview-ai>

Heilweil, R. (2020c, March 6). *The world's scariest facial recognition app company keeps lying*. Vox. <https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement>

Henning, K. (2013). Criminalizing normal adolescent behavior in communities of color: The role of prosecutors in juvenile justice reform. *Cornell Law Review*, 98(2), 383-461.

Herold, B. (2018, July 18). *Facial-recognition systems pitched as school-safety solutions, raising alarms*. Education Week. <https://www.edweek.org/ew/articles/2018/07/18/facial-recognition-systems-pitched-as-school-safety-solutions-ra.html>

Hill, K. (2020a, January 18). The secretive company that might end privacy as we know it. *The New York Times*. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

Hill, K. (2020b, March 5). Before Clearview became a police tool, it was a secret plaything of the rich. *The New York Times*. <https://www.nytimes.com/2020/03/05/technology/clearview-investors.html>

Holloway, H. (2019, August 12). Facial recognition cameras to track millions of people being rolled out across London. *Daily Star*. <https://www.dailystar.co.uk/news/latest-news/facial-recognition-cameras-london-canary-18924642>

Hoy, M. (2019, October 25). *Police use of facial recognition tech approved in Sweden*. Bloomberg Law. <https://news.bloomberglaw.com/privacy-and-data-security/police-use-of-facial-recognition-tech-approved-in-sweden>

Hugenberg, K., Young, S., Berstein, M., & Sacco, D. (2010). The categorization-individuation model: An integrative account of the other-race recognition deficit. *Psychological Review*, 117(4), 1168-1187. <https://doi.org/10.1037/a0020463>

Hunt, J. (2019) *From crime mapping to crime forecasting: the evolution of place-based policing*. National Institute of Justice Journal. <https://nij.ojp.gov/topics/articles/crime-mapping-crime-forecasting-evolution-place-based-policing>

H.R. 3875, 116th Cong. (2019)

Insler, C. N. (2018, December). How to tackle litigation under the Biometric Information Privacy Act. *The Computer & Internet Lawyer*, 35(12).

Introna, L. D., & Wood, D. M. (2002). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, 2(2/3), 177-198.

Jain, M. (2019, May 9). *The Aadhaar card: Cybersecurity issues with India's biometric experiment*. The Henry M. Jackson School of International Studies, University of Washington. <https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/>

James, B. (2015, March 2). *Stop and frisk in 4 cities: The importance of open police data*. Sunlight Foundation. <https://sunlightfoundation.com/2015/03/02/stop-and-frisk-in-4-cities-the-importance-of-open-police-data-2/>

Jarmanning, A. (2020, June 24). *Boston bans use of facial recognition technology*. It's the 2nd-largest city to do so. WBUR. <https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban>

Jin, L. (2019, September 5). *Science and Technology Department of the Ministry of Education: Campus promotion of face recognition technology should be cautious and will restrict and manage*. The Paper. https://www.thepaper.cn/newsDetail_forward_4343255

Jonson, C. L. (2017). Preventing school shootings: The effectiveness of safety measures. *Victims & Offenders*, 12(6), 956-973. <https://doi.org/10.1080/15564886.2017.1307293>

Kassin, S., Dror, I., & Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition*, 2(1), 42-52. <https://doi.org/10.1016/j.jarmac.2013.01.001>

Katz, L. R. (2004). Terry v. Ohio at thirty-five: a revisionist view. *Mississippi Law Journal*, 74(2), 423-500.

Kayali, L. (2019, October 29). French privacy watchdog says facial recognition trial in high schools is illegal. *Politico*. <https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/>

Kaye, D. (2019, June 25). *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools*. United Nations Human Rights Office of the High Commissioner. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736>

- Keval, H., & Sasse, M. A. (2010). "Not the usual suspects": A study of factors reducing the effectiveness of CCTV. *Security Journal*, 23(2), 134-154. <https://doi.org/10.1057/palgrave.sj.8350092>
- Kline, C. L. (2008). Security theater and database-driven information markets: A case for an omnibus U.S. data privacy statute. *University of Toledo Law Review*, 39(2), 443-496.
- Kobie, N. (2016, February 19). Surveillance state: Fingerprinting pupils raises safety and privacy concerns. *The Guardian*. <https://www.theguardian.com/sustainable-business/2016/feb/19/surveillance-state-fingerprinting-pupils-safety-privacy-biometrics>
- Kodali, S. (2019, September 28). Spying on your body: Health Blueprint and Aadhaar. *National Herald*. <https://www.nationalheraldindia.com/opinion/spying-on-your-body-health-blueprint-and-aadhaar>
- Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information (APPI)], Act No. 57 of May 30, 2003, as last amended by Act No. 51 of 2015.
- Kolkman, D. (2020). The (in)credibility of algorithmic models to non-experts. *Journal of Information, Communication, and Society*. <https://doi.org/10.1080/13669118X.2020.1761860>
- Kostka, G., Steinacker, L., & Meckel, M. (2020). Between privacy and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the UK and the US. *Social Science Research Network*. <http://dx.doi.org/10.2139/ssrn.3518857>
- Krimsky, S., & Simoncelli, T. (2010). *Genetic justice: DNA data banks, criminal investigations, and civil liberties*. New York: Columbia University Press.
- Kruse, C. (2015). *The social life of forensic evidence*. Oakland, CA: University of California Press.
- Kumar, A., & Bansal, M. (2015). Facial and voice recognition system using biometrics techniques. *International Journal for Innovative Research in Science & Technology*, 2(3), 14-17.
- Kuzma, J., Kokotovich, A., & Kuzhabekova, A. (2016). Attitudes towards governance of gene editing. *Asian Biotechnology and Development Review*, 18(1), 69-92.
- Lee, W., Wilkinson, C., Memon, A., & Houston, K. (2009). Matching unfamiliar faces from poor quality closed-circuit television (CCTV) footage: An evaluation of the effect of training on facial identification ability. *AXIS*, 1(1), 19-28.
- Leong, B. (2019). Facial recognition and the future of privacy: I always feel like ... somebody's watching me. *Bulletin of the Atomic Scientists*, 75(3), 109-115.
- Levine, D. (2007). Secrecy and unaccountability: Trade secrets in our public infrastructure. *Florida Law Review*, 59(1), 135-193. <https://ssrn.com/abstract=900929>

- Linder, T. (2019). Surveillance capitalism and platform policing: The surveillant assemblage-as-a-service. *Surveillance & Society*, 17(1/2), 76–82. <https://doi.org/10.24908/ss.v17i1/2.12903>
- Lopez, W. (2019). *Separated: Family and community in the aftermath of an immigration raid*. Baltimore, MD: Johns Hopkins University Press.
- Lum, C., Crafton, P. Z., Parsons, R., Beech, D., & Smarr, T. (2015, October). Discretion and fairness in airport security screening. *Security Journal*, 28(4), 352–373.
- Lum, K., & Isaac, W. (2016). To predict and serve? *In Detail*, 13(5), 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>
- Mackenzie, D. & Wajcman, J., eds. (1985). *The Social Shaping of Technology*. Philadelphia, PA: Open University Press.
- Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal*, 40(1), 121–145.
- Martineau, P. (2019, October 11). *Cities examine proper—and improper—uses of facial recognition*. *Wired*. <https://www.wired.com/story/cities-examine-proper-improper-facial-recognition/>
- McCarthy, J. (2017, August 24). *Indian Supreme Court declares privacy a fundamental right*. NPR. <https://www.npr.org/sections/thetwo-way/2017/08/24/545963181/indian-supreme-court-declares-privacy-a-fundamental-right>
- Nakamura, L., Samuels, J., & Soloveichik, R. (2017). *Measuring the ‘free’ digital economy within the GDP and productivity accounts*. Federal Reserve Bank of Philadelphia. <https://ssrn.com/abstract=3058017>
- National Center for Education Statistics. (2019). *School safety and security measures*. <https://nces.ed.gov/fastfacts/display.asp?id=334>
- National Institute of Standards and Technology. (2017, July 13). *Face recognition technology (FERET)*. <https://www.nist.gov/programs-projects/face-recognition-technology-feret>
- National Institute of Science and Technology. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects*. <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>
- Nelson, L., & Lind, D. (2015, February 24). *The school to prison pipeline, explained*. Justice Policy Institute. <http://www.justicepolicy.org/news/8775>
- New York Civil Liberties Union. (2020, July 22). *NYCLU statement on facial recognition in schools moratorium*. <https://www.nyclu.org/en/press-releases/nyclu-statement-facial-recognition-schools-moratorium>
- New York Civil Liberties Union. (n.d.b). *Legislative memo: Biometric identifying*

technology in schools. <https://www.nyclu.org/en/legislation/legislative-memo-biometric-identifying-technology-schools>

New York State's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, S. 5575B, 2019–2020 Legislative Session

No Biometric Barriers to Housing Act of 2019, H.R. 4008, 116th Cong. (2019)

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York, NY: Crown.

Parthasarathy, S. (2007). *Building genetic medicine: Breast cancer, technology, and the comparative politics of health care*. Cambridge, MA: MIT Press.

Parthasarathy, S. (2017). *Patent politics: Life forms, markets, and the public interest in the United States and Europe*. Chicago, IL: University of Chicago Press.

Paul, K. (2020, March 2). 'Ban this technology': Students protest US universities' use of facial recognition. *The Guardian*. <https://www.theguardian.com/us-news/2020/mar/02/facial-recognition-us-colleges-ucla-ban>

Perrigo, B. (2018, September 28). *India has been collecting eye scans and fingerprint records from every citizen. Here's what to know*. Time. <https://time.com/5409604/india-aadhaar-supreme-court/>

Perry, W., McInnis, B., Price, C., Smith, S., & Hollywood, J. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. RAND Corporation.

Personal Data Protection Bill, 2019. Parliament of India, Ministry of Law and Justice

President's Council of Advisors on Science and Technology. (2006). *Report to the President: Forensic science in criminal courts: Ensuring scientific validity of feature-comparison methods*. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf

Prictor, M., Teare, H. J. A., & Kaye, J. (2018). Equitable participation in biobanks: The risks and benefits of a "dynamic consent" approach. *Frontiers in Public Health*, 6, 1–6. <https://doi.org/10.3389/fpubh.2018.00253>

Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. AIES '19: *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*. 429–435.

Raviv, S. (2020, January 21). *The secret history of facial recognition*. Wired. <https://www.wired.com/story/secret-history-facial-recognition/>

Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice.

New York University Law Review, 94, 192–233. <https://ssrn.com/abstract=3333423>

Ripley, A. (2016). *How America outlawed adolescence*. The Atlantic. <https://www.theatlantic.com/magazine/archive/2016/11/how-america-outlawed-adolescence/501149/>

Robinson, C. (2018, August 20). *Here's how much school security has changed, increased over the past 20 years*. WTSP. <https://www.wtsp.com/article/news/education/heres-how-much-school-security-has-changed-increased-over-the-past-20-years/67-585889537>

Rogers, K. (2016, February 7). *That time the Super Bowl secretly used facial recognition software on fans*. Vice. https://www.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans

Rosenzweig, P., Kochems, A., & Schwartz, A. (2004). *Biometric technologies: Security, legal, and policy implications*. The Heritage Foundation. <https://www.heritage.org/homeland-security/report/biometric-technologies-security-legal-and-policy-implications>

Ross, J. (2016, December). *Warning: Stop-and-frisk may be hazardous to your health*. *The William and Mary Bill of Rights Journal*, 25(2), 689–733.

SAFR. (n.d.). *SAFR for K–12 schools: Introducing SAFR facial recognition for K–12 schools*. <https://safr.com/k12/>

Samuel, S. (2020, January 29). *Is your college using facial recognition on you? Check this scorecard*. Vox. <https://www.vox.com/2020/1/29/21112212/facial-recognition-college-campus-scorecard>

Sankar, P., & Parker, L. S. (2013). Precision Medicine Initiative's All of Us Research Program: An agenda for research on its ethical, legal, and social issues. *Genetics in Medicine*, 19(7), 743–750.

Scheck, B., Neufeld, P., & Dwyer, J. (2003). *Actual innocence: When justice goes wrong and how to make it right*. New York, NY: Signet.

Scheuerman, M. K., Paul, J. M., & Brubaker, J. R. (2019). How computers see gender: An evaluation of gender classification in commercial facial analysis and image labeling services. *Proceedings of the ACM on Human-Computer Interaction*, 3. <https://dl.acm.org/doi/10.1145/3359246>

Security services 'prevented 13 UK terror attacks since 2013'. (2017, March 6). BBC News. <https://www.bbc.com/news/uk-39176110>

Selin, C. (2011). Negotiating plausibility: Intervening in the future of nanotechnology. *Science and Engineering Ethics*, 17, 723–737.

Sergeant Shiver National Center on Poverty Law. (2017). *Handcuffs in hallways: The state of policing in Chicago public schools*. <https://www.povertylaw.org/article/handcuffs-in-hallways-the-state-of-policing-in-chicago-public-schools/>

- Sewell, A. A., Jefferson, K. A., & Lee, H. (2016). Living under surveillance: Gender, psychological distress, and stop-question-and-frisk policing in New York City. *Social Science & Medicine*, 159, 1-13.
- Short, C. (2007). Guilt by machine: The problem of source code discovery in Florida DUI prosecutions. *Florida Law Review*, 61(1), 177-201.
- Should government halt the use of facial-recognition technology?* (2020, February 23). The Wall Street Journal. <https://www.wsj.com/articles/should-government-halt-the-use-of-facial-recognition-technology-11582513260>.
- Simonite, T. (2020, May 1). *How Well Can Algorithms Recognize Your Masked Face?* Wired. <https://www.wired.com/story/algorithms-recognize-masked-face/>
- Simonite, T., & Barber, G. (2019, October 17). *The delicate ethics of using facial recognition in schools.* Wired. <https://www.wired.com/story/delicate-ethics-facial-recognition-schools/>
- Singer, N. (2019, January 24). Amazon is pushing facial technology that a study says could be biased. *The New York Times*. <https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html>
- Singh, S. (2019). *Facial recognition market worth \$7.0 billion by 2024.* Markets and Markets. <https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp>
- Smith, S. M., Stinson, V., & Prosser, M. A. (2004). Do they all look alike? An exploration of decision-making strategies in cross-race facial identifications. *Canadian Journal of Behavioural Science*, 36, 144-153. <https://doi.org/10.1037/h0087225>
- Snow, J. (2020, February 10). *Hey Clearview, your misleading PR campaign doesn't make four face surveillance product any less dystopian.* American Civil Liberties Union. <https://www.aclu.org/news/privacy-technology/hey-clearview-your-misleading-pr-campaign-doesnt-make-your-face-surveillance-product-any-less-dystopian/>
- Spaun, N. A. (2011). Face recognition in forensic science. In: S. Z. Li & A. K. Jain. (Eds.) *Handbook of face recognition.* Springer-Verlag London.
- Spitzer, E. (1999). *The New York City police department's stop and frisk practices: A report to the people of the State of New York from the Office of the Attorney General.* The Office of the Attorney General of the State of New York, Civil Rights Bureau.
- Spriggs, A., Argomaniz, J., Gill, M., & Bryan, J. (2005). *Public attitudes towards CCTV: Results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV.* Home Office. <http://library.college.police.uk/docs/hordsolr/rdsolr1005.pdf>

- Steinsbekk, K. S., Myskja, B. K., & Solberg, B. (2013). Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem? *European Journal of Human Genetics*, 21(9), 897–902. <https://doi.org/10.1038/ejhg.2012.282>
- Stilgoe, J., Owen, R., & Macnaughten, P. (2013). Developing a framework for responsible innovation. *Research Policy*, 42(9), 1568–1580. <https://doi.org/10.1016/j.respol.2013.05.008>
- Stirling, A. (2008). 'Opening up' and 'closing down': Power, participation, and pluralism in the social appraisal of technology. *Science, Technology, and Human Values*, 33(2), 262–294.
- Sutton, H. (2019). Report finds department abused facial recognition software. *Campus Security Report*, 16(4), 1–12. <https://doi.org/10.1002/casr.30546>
- Symanovich, S. (n.d.). *How does facial recognition work?* Norton. <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html>
- Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. *IEEE Conference on Computer Vision and Pattern Recognition*, 1701–1708. <https://doi.org/10.1109/CVPR.2014.220>
- Taylor, E. (2010). I spy with my little eye: The use of CCTV in schools and the impact on privacy. *The Sociological Review*, 58(3), 381–405.
- Taylor, E. (2011). UK schools, CCTV and the Data Protection Act 1998. *Journal of Education Policy*, 26(1), 1–15.
- Taylor, E. (2013). *Surveillance schools: Security, discipline and control in contemporary education*. Palgrave Pivot.
- The Consentful Tech Project. (n.d.). *What is consentful tech?* <https://www.consentfultech.io/>
- The history of CCTV*. (2015, November 4). Herring Technology. <https://herringtechnology.com/news/the-history-of-cctv/>
- The Public Voice. (2019, October). *Declaration: A moratorium on facial recognition technology for mass surveillance*. <https://thepublicvoice.org/ban-facial-recognition/>
- The State of New Hampshire v. William Joseph Sullivan, Jr., N.H. 2005–594 (2008)
- Thorat, S. B., Nayak, S. K., & Dandale, J. P. (2010). Facial recognition technology: An analysis with scope in India. *International Journal of Computer Science and Information Security*, 8(1), 325–330.
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134–153.
- Todd, R. (2020, February 7). *Google hit with class action under Illinois Biometric*

- Privacy Law over facial recognition.* The Recorder. <https://www.law.com/therecorder/2020/02/07/google-hit-with-class-action-under-illinois-biometric-privacy-law-over-facial-recognition/>
- Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1), 71-86.
- Turner, A., Dailaire-Fortier, C., & Murtagh, M. J. (2013). Biobank economics and the “commercialization problem”. *Spontaneous Generations: A Journal for the History and Philosophy of Science*, 7(1), 69-80.
- 210 govt. websites made Aadhaar details public: UIDAI. (2017, November 19). The Hindu. <https://www.thehindu.com/news/national/210-govt-websites-made-aadhaar-details-public-uidai/article2055266.ece>
- Ulery, B., Hicklin, R., Buscaglia, J., & Roberts, M. (2012). Repeatability and reproducibility of decisions made by latent fingerprint examiners. *PLoS ONE*, 7(3), 1-12. <http://dx.doi.org/10.1371/journal.pone.0032800>
- Ulery, B., Hicklin, R., Roberts, M., & Buscaglia, J. (2014). Measuring what latent fingerprint examiners consider sufficient information for individualization determinations. *PLoS ONE*, 9(11). <https://doi.org/10.1371/journal.pone.0110179>
- Ulle, M. (2019, August 15). *How are states responding to facial recognition surveillance?* Project on Government Oversight. <https://www.pogo.org/analysis/2019/08/how-are-states-responding-to-facial-recognition-surveillance/>
- US Department of Education. (2018, March 1). *Family Educational Rights and Privacy Act (FERPA)*. <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- Valentino-Devries, J. (2019, April 13). Tracking phones, Google is a dragnet for the police. *The New York Times*. www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html
- Valentino-DeVries, J. (2020, January 12). How the police use facial recognition, and where it falls short. *The New York Times*. <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>
- Villalobos, J., & Davis, D. (2016). Interrogation and the minority suspect: Pathways to true and false confession. In M. Miller & B. Bornstein (Eds.), *Advances in Psychology and Law* (Vol. 1) (pp.1-42). Cham, Switzerland: Springer Nature.
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing.
- Webster, W. (2009). CCTV policy in the UK: Reconsidering the evidence base. *Surveillance & Society*, 6(1), 10-22. <https://doi.org/10.24908/ss.v6i1.3400>

Weise, K., & Singer, N. (2020, June 10). Amazon pauses police use of its facial recognition software. *The New York Times*. <https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html>

Welsh police wrongly identify thousands as potential criminals. (2018, May 5). *The Guardian*. <https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals>

West, D. M. (2019). *10 actions that will protect people from facial recognition software.* The Brookings Institution. <https://www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/>

Woodward, J. D. (2001). Super Bowl surveillance: Facing up to biometrics. *RAND Corporation*, 3-16.

Yan, L. (2019, November 28). *China eyes 'ethical' facial recognition standard.* Ecns. <http://www.ecns.cn/m/news/sci-tech/2019-11-28/detail-ifzrhrks8236651.shtml>

Zeide, E. (2017). Student privacy principles for the age of big data: Moving beyond FERPA and FIPPs. *Drexel Law Review*, 8(2), 101-160.

Zuboff, S. (2018). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* London, United Kingdom: Profile Books.

Further Resources

Reports & Articles

“Ban Biometric Mass Surveillance: a set of fundamental rights demands for the European Commission and EU Member States”, *European Digital Rights* (2020).

“Biometric Technologies: Security, Legal, and Policy Implications” by Paul Rosenweig, Alane Kochems, and Ari Schwartz, *The Heritage Foundation* (2004).

“Biometrics and Children: A literature review of current technologies”, *UNICEF and the World Bank Group* (forthcoming).

“Face Recognition Policy Development Template”, *Bureau of Justice Assistance*, US Department of Justice & US Department of Homeland Security (2017).

“Faces, Fingerprints & Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs”, *UNICEF* (2019).

“Facial Recognition Technology: A Survey of Policy and Implementation Issues” by Lucas D. Introna and Helen Nissenbaum, *The Center for Catastrophe Preparedness & Response*, New York University (2009).

“Privacy Principles for Facial Recognition Technology in Commercial Applications”, *Future of Privacy Forum* (2018).

“Understanding Facial Recognition Systems”, *Partnership on AI* (2020).

“10 actions that will protect people from facial recognition software” by Darrell M. West, *The Brookings Institution* (2019).

Think Tanks & Civil Society Groups Working on FR

[Access Now](#)

[American Civil Liberties Union](#)

[Bits of Freedom](#)

[Center for Democracy & Technology](#)

[Electronic Frontier Foundation](#)

[Electronic Privacy Information Center](#)

[European Digital Rights](#)

[Digitale Gesellschaft](#)

[Drzavljan D](#)

[Fight for the Future](#)

[Future of Privacy Forum](#)

[Georgetown Center on Privacy & Technology](#)

[Homo Digitalis](#)

[La Quadrature du Net](#)

[New York Civil Liberties Union](#)

[Open Rights Group](#)

[Partnership on AI](#)

[The Brookings Institution](#)

[The Heritage Foundation](#)

[The Information Technology and Innovation Foundation](#)

[The Public Voice](#)

[UNICEF AI for Children](#)

[UNICEF Generation AI](#)

Appendix A

Questions for School Administrators and Teachers to Ask Facial Recognition Companies

ACCURACY OF THE TECHNOLOGY

- What are the false positive and false negative rates for the technology (For a definition of false positives and negatives, see [p. 18](#))?
- How is the accuracy of your algorithm determined? Is it validated externally?
- Is the accuracy of the algorithm the same across demographic groups including children?
- Where does the data that informs the algorithm come from?
- What steps does your company take to ensure that the technology does not have disparate impacts, particularly among vulnerable populations?

DATA MANAGEMENT PRACTICES

- Can we prevent data collection from students' social media accounts?
- How frequently will data be deleted?
- Where/how will data be stored? What are the protections on data?
- Can students opt-out of the technology? How?

OPERATING FACIAL RECOGNITION IN SCHOOLS

- How should the technology be deployed and used, and what human and technological resources will we need, in order to ensure ongoing accuracy?
- How does the technology need to be maintained, and how frequently should this occur? What are the maintenance costs for the technology?
- What types of cameras do we need to use to ensure accurate results? How much do they cost? Will they be managed by the same company as the software, or separately?

Appendix B

Questions for Parents, Guardians, and Students to Ask Schools and School Districts

GENERAL QUESTIONS

- Why is this technology needed? Why were alternatives to facial recognition unacceptable?
- How and when will the technology be used?
- How will you ensure the technology is not used beyond its original intended purpose?
- How will the technology's utility be evaluated over time?
- How will parents, guardians, and students be involved in making decisions about how and when the technology is used?
- What experts were consulted in deciding to adopt facial recognition?
- Particularly for parents and guardians of younger students: how should I describe facial recognition use to my child?
- Where can I find additional resources about facial recognition to learn more?

ACCURACY OF THE TECHNOLOGY

- What are the false positive and false negative rates for the technology?
- How is the accuracy of the algorithm determined? Is it validated externally?
- What cameras are you using, and how do we know they are producing accurate results?
- What data is collected?
- Where does the data used to train the algorithm come from?
- Is the accuracy of the algorithm the same across demographic groups including children?
- Can we prevent data collection from students' social media accounts?
- How frequently will data be deleted?
- Where and how will data be stored? What are the protections on data?
- How will the technology be maintained, and how frequently?

USE IN SCHOOLS

- Does the school have the proper infrastructure and personnel to use the technology appropriately?
- How will the school determine who is on a watch list, and how will that determination be made?
- Under what circumstances will the facial recognition system be used to discipline students?
- How will you prevent use of the technology for behavioral monitoring?
- How will the use of facial recognition for student discipline be monitored and evaluated for evidence of bias, both systemic and individual? What consequences will be associated with facial recognition identifications? What appeals will be available?
- What is the response plan after an unauthorized visitor is identified?
- Can we opt-out of participating in the system? How?
- How will the operators of the technology be trained?
- How will operators avoid racial, ethnic, and gender bias?
- Who will have access to student data and match results? How will this be limited?
- Where in the school will be cameras be deployed?

For Further Information

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

© 2020 The Regents of the University of Michigan