ARTICLE

BAN FACIAL RECOGNITION TECHNOLOGIES FOR CHILDREN—AND FOR EVERYONE ELSE

LINDSEY BARRETT[*]

Abstract

Facial recognition technologies enable a uniquely dangerous and pervasive form of surveillance, and children cannot escape it any more than adults can. Facial recognition technologies have particularly severe implications for privacy, as they can weaponize existing photographic databases in a way that other technologies cannot, and faces are difficult or impossible to change, and often illegal to publicly obscure. Their erosion of practical obscurity in public threatens both privacy and free expression, as it makes it much harder for people to navigate public spaces without being identified, and easier to quickly and efficiently identify many people in a crowd at once. To make matters even worse, facial recognition technologies have been shown to perform less accurately for people of color, women, non-binary and transgender people, children, and the elderly, meaning that they have the potential to enable discrimination in whatever forum they are deployed. As these technologies have developed and become more prevalent, children are being subjected to it in schools, at summer camp, and other child-specific contexts, as well as alongside their parents, through CCTV, private security cameras, landlord-installed apartment security systems, or by law enforcement.

The particular vulnerability of young people relative to adults might make them seem like natural candidates for heightened protections from facial recognition technologies. Young people have less say over where they go and what they do, inaccurate evaluations of their faces could have a particularly strong impact on their lives in contexts like law enforcement uses, and the chilling effects of these technologies on free expression could constrain their emotional and intellectual development. At the same time, some of the harms young people experience are near-universal privacy harms, such as the erosion of practical

[*] Staff Attorney and Teaching Fellow, Communications and Technology Law Clinic, Georgetown University Law Center. Enormous thanks to Laura Moy, Woody Hartzog, Amanda Levendowski, Os Keyes, Joe Jerome, Tiffany Li, Meg Leta-Jones, and Michael Rosenbloom for their tremendously thoughtful feedback—errors, as always, entirely mine.

obscurity, while the discriminatory harms of facial recognition's inaccurate assessment of their faces are shared by other demographic groups.

The dangers facial recognition technologies pose to human flourishing are insidious enough that a ban on both commercial and government uses is necessary, as more modest proposals will likely be insufficient to counteract their inescapability and discriminatory effects. But children's heightened vulnerability to privacy violations and discrimination from the use of facial recognition technologies doesn't diminish the severity of the harms that other groups and the population at large experience. The use of facial recognition technologies on children should be prohibited, and the same goes for their use on everyone else.

INTRODUCTION

In a world where commercial and governmental surveillance have crept into so many aspects of daily life, facial recognition technologies pose a particularly severe risk to privacy, free expression, fairness, and other democratic values. The simple fact that you can reset a password, but not your face, heightens the stakes of using faces as an identifier; it makes surveillance systems harder to evade, and breaches more consequential. Facial recognition enables the government or corporate entities to quickly and cheaply survey a crowd and isolate individuals from it, which eats away at practical obscurity. People provide (or are required to provide) identification pictures to government agencies and private entities every day, for a range of reasons, and the existence of these databases means that facial recognition makes them perpetually the possible subject of automated evaluation. If all of that weren't frightening enough, researchers have repeatedly demonstrated that facial recognition systems are often less accurate for people of color, women, non-binary individuals, and young people.[1] Every circumstance in which facial recognition is deployed—by banks, by companies assessing job applicants, by government agencies identifying people, by private security companies, by law enforcement agents searching for suspects—creates new opportunities for members of those groups to be discriminated against.

The use of facial recognition technologies on children is fraught with competing motivations and concerns, given the broad consensus that children are a vulnerable population in need of heightened protections,[2] and the lack of consensus over the primary sources of threats to them and how best to mitigate those threats.[3] Facial recognition technologies bring this conflict to a head, as the collective impulse to protect children comes into conflict with what they need to be

[1] Steve Lohr, *Facial Recognition is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 8, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/HK9M-WVED]; *see also* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 6:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [https://perma.cc/TW4J-NMRN].

[2] *See, e.g.*, G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) ("Motherhood and childhood are entitled to special care and assistance. All children, whether born in or out of wedlock, shall enjoy the same social protection.").

[3] *See* Toni Smith-Thompson, *Here's What Happens When We Allow Facial Recognition Technology in Our Schools*, ACLU (Aug. 15, 2018, 11:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/heres-what-happens-when-we-allow-facial [https://perma.cc/39DQ-YNQH] (detailing harms of facial recognition use in schools and possible solutions to protect children); Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App is Identifying Child Victims of Abuse*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html [https://perma.cc/CV89-Y7NF] ("We understand the extreme sensitivity involved with identifying children.").

protected from: the dangerous actors whose conduct concerning surveillance is often intended to avert, or the harms to privacy, free expression, and self-determination that surveillance itself inflicts. For facial recognition technologies to be a net good for children's safety, they would have to be more accurate than they are, less discriminatory than they are on the basis of race, gender, and age, and their impact on privacy, free expression, and due process less severe.

But those problems remain, making the use of facial recognition on children at least as damaging as whatever lurking dangers the surveillance itself promises to prevent. The deployment of facial recognition systems in child-centric locations like schools and summer camps is unlikely to deliver the improved safety that facial recognition vendors assure, while putting children's privacy at risk. Children are also often subjected to the same forms of general, non-child-specific uses of facial recognition technologies as their parents. Teenagers and even young children are active users of social media applications that deploy facial recognition technologies, like Facebook and Instagram.[4] They also frequent public and private spaces that are subject to facial recognition-fueled surveillance, such as churches,[5] concerts,[6] or public protests.[7] Like adults, children may also be surveilled by law enforcement.[8] We don't fully understand how children will react to real-time surveillance of their movements when they're aware of it occurring and understand the ramifications, and know that they endanger their privacy when they don't fully understand the risks. What's more, the inaccuracy of these systems in identifying young people and people of color introduces new forms of chaos and possible discrimination when the technology doesn't work the way it's supposed to.

[4] *See* Alice Marwick & Danah Boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051, 1052, 1062 (2014); Alfred Ng, *Your Face Mask Selfies Could Be Training the Next Facial Recognition Tool*, CNET (May 19, 2020, 5:00 AM), https://www.cnet.com/news/your-face-mask-selfies-could-be-training-the-next-facial-recognition-tool/ [https://perma.cc/W5A2-UNSZ].

[5] *Facial Recognition Software by Churchix for Biometric Attendance,* CHURCHIX, https://churchix.com/ [https://perma.cc/7XM5-CBEV].

[6] *See* Gabrielle Canon, *How Taylor Swift Showed us the Scary Future of Facial Recognition*, THE GUARDIAN (Feb. 15, 2019), https://www.theguardian.com/technology/2019/feb/15/how-taylor-swift-showed-us-the-scary-future-of-facial-recognition [https://perma.cc/QHE2-MCY5].

[7] Rina Chandran, *Use of Facial Recognition in Delhi Rally Sparks Privacy Fears*, REUTERS (Dec. 30, 2019, 6:31 AM), https://www.reuters.com/article/us-india-protests-facialrecognition-trfn/use-of-facial-recognition-in-delhi-rally-sparks-privacy-fears-idUSKBN1YY0PA [https://perma.cc/SCZ2-QSJM].

[8] Joseph Goldstein & Ali Watkins, *She was Arrested at 14. Then her Photo went to a Facial Recognition Database*, N.Y. TIMES (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html [https://perma.cc/5C6Q-2L8Z] (explaining use of facial recognition surveillance on children by New York City law enforcement).

The rapid spread of facial recognition technologies and their accompanying harms leaves the question of how the law should respond. Certain laws in the United States that are specific to the use of biometrics, and specific to children's privacy, provide certain protections, but are still insufficient to mitigate the damage or prevent more of it. For example, three state laws that govern the use of biometrics in Illinois, Texas, and Washington state offer some protections.[9] However, these laws are ultimately too heavily tied to a "notice and choice" method of privacy governance, a paradigm that is particularly poorly suited to a system of surreptitious surveillance which relies on an identifier that's hard to hide, hard to change, and often included in a database either because of legal or practical requirements or without the person's knowledge. These laws are also limited in geographic and subject-matter jurisdiction, and under-enforced.

Child-specific privacy laws are similarly insufficient to protect children from the harms of facial recognition technologies. The Children's Online Privacy Protection Act (COPPA), like the state biometrics laws, also relies heavily on a failed notion that a privacy policy can ensure privacy protections. And while some of COPPA's requirements may make certain general audience uses of the technology untenable, the law is also under-enforced, only reaches companies in the Federal Trade Commission's jurisdiction, and only applies to children under the age of 13.[10] The Family Educational Rights and Privacy Act (FERPA), which curbs the ability of schools to share students' educational records,[11] is similarly limited and under-enforced. None of these laws go far enough to protect the privacy risks that the use of facial recognition technologies on children presents, and none of them will prevent its spread into various parts of young people's lives. Indeed, they are not designed to diminish the use of technology on children at all.[12]

[9] *See* Michael A. Rivera, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 571, 576 (2019); Jennifer J. Froehlich, *New Illinois Law Governs Use of Artificial Intelligence During Interview Process*, HOLLAND & KNIGHT (Aug. 12, 2019), https://www.hklaw.com/en/insights/publications/2019/08/new-illinois-law-governs-use-of-artificial-intelligence [https://perma.cc/YS2A-HDUF].

[10] *See* Tony Romm & Craig Timberg, *Federal Regulators Eye Update to Rules Governing Children's Privacy and the Internet*, WASH. POST (July 18, 2019, 10:55 AM), https://www.washingtonpost.com/technology/2019/07/18/federal-regulators-eye-update-rules-governing-kids-privacy-internet/ [https://perma.cc/47YQ-FWDT] (explaining COPPA's limitations).

[11] Willard Dix, *You Need to Understand Your Educational Privacy Rights*, FORBES (May 16, 2018, 11:54 AM), https://www.forbes.com/sites/willarddix/2018/05/16/you-need-to-understand-your-educational-privacy-rights/#7cf6eae96b93 [https://perma.cc/4R86-2C98].

[12] COPPA was intended to protect children's privacy without halting the growth of the market for online services. *See* Press Release, FTC, New Rule to Protect Children's Online Privacy Takes Effect April 21, 2000 (Apr. 20, 2000), https://www.ftc.gov/news-events/press-releases/2000/04/new-rule-protect-childrens-online-privacy-takes-effect-april-21

Consternation about the increasingly rapid deployment of these discriminatory and privacy-invasive technologies without meaningful safeguards has drawn a number of proposals to regulate their use. The most permissive proposals argue that the benefits of facial recognition technologies as surveillance tools, their utility for governmental investigators, and the added ease and efficiency of the commercial applications support hands-off rules that would facilitate, rather than prevent, the deployment of these technologies.[13] The more expansive proposals include a moratorium on the use of facial recognition technologies until the bias problems can be corrected (if that's even possible), with strict privacy safeguards like data use limitations. The most aggressive of these proposals is a comprehensive ban on the use of facial recognition technologies, given their almost unique inescapability, and the fact that the possibility these services will ever be sufficiently unbiased is far from guaranteed. Many of the more permissive proposals come from technology companies, or non-profits and trade associations aligned with them; advocates and privacy scholars have generally proposed or supported more aggressive proposals.[14]

[https://perma.cc/N69C-Y498] (stating that COPPA includes "safe harbor" provision to encourage industry self-regulation); Elana Zeide, *The Limits of the Education Purpose Limitations*, 71 U. MIAMI L. REV. 494, 498 (2017) (describing FERPA as intended to provide greater "transparency and confidentiality" over schools' processing of students' information).

[13] *See, e.g.,* Hearing on "Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy" Before the H. Comm. on Oversight and Reform, 116th Cong. 11-12 (2020) [hereinafter *Hearing on Facial Recognition Technology*] (statement of Daniel Castro, Vice President and Director of Center for Data Innovation, Information Technology and Innovation Foundation); Daniel Castro, *No, Government Should Not Halt the Use of Facial-Recognition Technology*, INFO. TECH. & INNOVATION FOUND. (Feb. 23, 2020), https://itif.org/publications/2020/02/23/no-government-should-not-halt-use-facial-recognition-technology [https://perma.cc/QF4R-T8ZY]; *Facial Recognition Policy Principles*, U.S. CHAMBER OF COM. TECH. ENGAGEMENT CTR. (last visited June 22, 2020), https://www.uschamber.com/sites/default/files/ctec_facial_recognition_policy_principles_002.pdf [https://perma.cc/V46P-3JKQ] (urging policymakers to prioritize "transparent use"); Matthew Feeney, *Facial Recognition Technology is Getting Out of Control*, CATO INST. (Mar. 9, 2020), https://www.cato.org/publications/commentary/facial-recognition-technology-getting-out-control [https://perma.cc/Z77S-2QJT] (arguing for "A liberal approach to facial recognition that respects civil liberties without being technophobic"); Alan McQuinn, *Don't Demonize Facial Recognition Technology, Establish Rules and Norms for Its Use*, INFO. TECH. & INNOVATION FOUND. (May 24, 2018), https://itif.org/publications/2018/05/24/dont-demonize-facial-recognition-technology-establish-rules-and-norms-its [https://perma.cc/J6LD-E9AD]; Adam Thierer, *The Great Facial Recognition Technopanic of 2019*, THE BRIDGE (May 17, 2019), https://www.mercatus.org/bridge/commentary/great-facial-recognition-technopanic-2019 [https://perma.cc/LQ5E-58ES] ("[I]nstead of a flat ban, we should prohibit real-time facial recognition tracking by governments while allowing its use as an ex post investigative tool.").

[14] *See generally* Woodrow Hartzog, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/H27B-L4LZ] (proposing outright ban on use

To my knowledge, there haven't been many calls for child-specific facial recognition protections.[15] But children are a sympathetic population, and their privacy protections often draw a broader consensus than do protections for adults given the general agreement that children's immaturity makes them particularly vulnerable in a variety of ways. The combination of a rising tide of facial recognition regulation with its frequent use on a population whose privacy rights are more widely agreed upon as necessary raises the question. What would be the value of a child-specific ban on the use of these technologies?

Children's developmental immaturity, their even weaker ability to avoid unwanted surveillance relative to adults, and the fact that facial recognition technologies are generally less accurate for them might seem to support a uniquely high standard, like a child-specific ban on facial recognition technologies. Some of the harms may be particularly severe for children, others are shared by other demographic groups or are nearly universal. The possible harms ensuing from facial recognition technologies' limited ability to accurately recognize young faces are similar to those shared by other demographic groups, such as people with darker skin, Asian people, non-binary people, and the elderly. Facial recognition's erosion of practical obscurity is a broadly shared harm, as is the erosion of due process protections in law enforcement investigations and the chilling effect on political protest.

But even if a child-specific ban were morally defensible or a sufficient response to the full range of implicated threats, it would also be near-impossible to meaningfully enact. Young people are often subjected to general-audience

of facial recognition technology); Barry Friedman & Andrew Guthrie Ferguson, *Here's a Way Forward on Facial Recognition*, N.Y. TIMES (Oct. 31, 2019), https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html [https://perma.cc/9WTM-HFP8] (proposing a ban on facial surveillance while allowing police face identification); *ACLU Comment on Microsoft Call for Federal Action on Face Recognition Technology*, ACLU (July 13, 2019), https://www.aclu.org/press-releases/aclu-comment-microsoft-call-federal-action-face-recognition-technology [https://perma.cc/4WE9-UVJK] (agreeing with Microsoft that "face recognition use by law enforcement must be fully analyzed and debated). *But see* Judith Donath, *You are Entering an Ephemeral Bio Allowed Data Capture Zone*, MEDIUM (July 23, 2018), https://medium.com/@judithd/you-are-entering-an-ephemeral-bio-allowed-data-capture-zone-5ecafd2dbdaf [https://perma.cc/9KR2-PR29] (arguing that facial recognition technologies should be regulated, not banned).

[15] *Cf.* Mark Andrejevic & Neil Selwyn, *Facial Recognition Technology in Schools: Critical Questions and Concerns*, 45 LEARNING, MEDIA & TECH. 115, 124-26 (2019) ("In terms of [the othering, oppression and coercive control that facial recognition technology inflicts], it makes little sense for students (and teachers) to actively work to legitimize inhumane forms of datafied schooling . . . is this a form of digital technology that should not be 'educationally' applied in any form whatsoever?"); Russell Brandom, *How Should We Regulate Facial Recognition?*, THE VERGE (Aug 29, 2018, 10:13 AM), https://www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules [https://perma.cc/B5FK-UB5Y] ("You probably want protections for children. It should probably not be used on people who are 18 or younger.").

uses of these technologies, which will make parsing legal and illegal uses difficult. In this article, I argue that in some ways, the harms of facial recognition technologies are particularly severe for children, but only slightly more so than they are for a number of distinct groups, and for the population as a whole. The damage caused by facial recognition technologies to fundamental freedoms and their fundamental inescapability warrant a comprehensive ban on their use. The severity of that damage for children simply adds additional support for the case.

This article proceeds in six parts. Part II describes how facial recognition technologies are being deployed by private entities and law enforcement, and used on adults and children alike. Part III describes the harms to privacy and free expression that facial recognition technologies impose, as well as their potential to cause or exacerbate discrimination, and explain which of these harms are particularly severe for children, which are shared by other demographic groups, and which are quasi-universal. Part IV describes the inadequacy of the existing legal protections that apply to the use of facial recognition technologies, illustrating why a ban would not be superfluous. Part V explains why a comprehensive ban is needed and why a child-specific ban would be undesirable. Part VI addresses further considerations and Part VII concludes.

USES OF FACIAL RECOGNITION TECHNOLOGIES

The various uses of facial recognition technologies can often sound like science fiction, which makes their dystopian implications all the more fitting.[16] As more and more entities have turned to these technologies and they become cheaper and more accurate, they also become harder to evade.

How the Technology Works

Different applications of the technology are better suited for particular uses, and understanding each component and application is crucial to understanding what the technology can accomplish and the harms it can inflict. "Facial recognition technology" generally describes the automated detection of a face for analyzing it, whether for identification or classification of various other attributes.[17] Generally, this process involves creating an algorithm to assess facial

[16] *See* Lane Brown, *There Will be No Turning Back on Facial Recognition*, N.Y. MAG. (Nov. 12, 2019), http://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html [https://perma.cc/J2BQ-H8F3]; Charlie Warzel, *All this Dystopia, and for What?*, N.Y. TIMES (Feb 18, 2020), https://www.nytimes.com/2020/02/18/opinion/facial-recognition-surveillance-privacy.html [https://perma.cc/9QM9-TEPC] (explaining how the use of facial recognition technology in many situations causes a "troubling dystopia—one full of false positives, confusion and waste.").

[17] CLARE GARVIE ET AL., THE PERPETUAL LINE-UP 9 (Georgetown Law, Center on Privacy and Technology 2016); *see also* ERIK LEARNED-MILLER ET AL., FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE 3 (2020) ("Borrowing from the Federal Trade Commission [1], we use the term "facial recognition technologies" as a catchall phrase to describe a set of technologies that process imaging data to perform a range of tasks

images (including 'training' it on a databases of faces, in the case of a machine learning algorithm); creating a template database of faces that the algorithm will use to compare new images against; and then comparing probe images to the template database. In order to assess the probe image, the algorithm detects whether a face exists in an image, then breaks the image into features (such as the eyes, nose, mouth), and the distance between them, so that they can be numerically quantified in a template.[18]

Depending on how the program is designed, the algorithm might provide a range of possible matches or one match with some kind of measurement of the algorithm's confidence that the person has been correctly identified.[19] Some systems, including Amazon's Rekognition, permit the user to evaluate the level of confidence—ostensibly indicating the likelihood that the image is a match, though in the case of Amazon Rekognition, the company has been unhelpfully opaque regarding the metrics used.[20] The quality of the image has a tremendous impact on the ability of the algorithm to assess it—factors like low image resolution, poor lighting, and whether the face is twisted or obscured all render the algorithm less likely to be able to detect the face or identify to whom it belongs.[21]

In the case of facial recognition algorithms that rely on machine learning, the size and variety of the dataset the algorithm is trained on impacts the accuracy of the algorithm. An algorithm that "learns" what a face is supposed to look like by training on a dataset predominantly composed of images from one particular demographic, such as white men, will tend to perform less accurately for other groups whose faces do not resemble what the algorithm has been built to interpret as a "face."[22] The same holds true for the size and heterogeneity of a database used as part of a "benchmark, " or a test intended to measure the accuracy

on human faces, including detecting a face, identifying a unique individual, and estimating demographic attributes.").

[18] *Id.*; Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1, 5-6 (forthcoming); *Face Recognition*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/face-recognition [https://perma.cc/U7ER-26EE].

[19] *Face Recognition*, *supra* note 18.

[20] *See Amazon Rekognition FAQs,* AMAZON, https://aws.amazon.com/rekognition/faqs/ [https://perma.cc/GR6D-2FPM] (discussing what a "confidence score" is and how to use it).

[21] *Face Recognition*, *supra* note 18; *see* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/C3JF-ACPQ] (citing to a white paper "titled 'Facial Recognition: Art or Science?' published by the company Vigilant Solutions that posits that face recognition systems—even without considering composite sketches—are '[p]art science and part art'").

[22] GARVIE ET AL., *supra* note 17; *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy: Hearing Before H. Comm. on Oversight and Gov't Reform*, 116th Cong. 2 (2020) (testimony of Charles Romine, Director, Information Technology Laboratory).

of a facial recognition system as applied to a certain task or under certain circumstances.[23] If the database that the system is tested on only contains photographs of faces with, for example, a certain skin color, or of a certain age, the test will not reflect how well the facial recognition system will perform on faces that do not share those attributes.

Different kinds of searches have different uses. "One-to-one" matching, or facial verification, describes when an algorithm verifies the identity of the subject by comparing the test image to an image of the subject, rather than attempting to ascertain the subject's unknown identity.[24] Many commercial uses of facial verification, such as the Face ID on an Apple iPhone[25] or user verification in mobile banking applications,[26] rely on one-to-one matching. In contrast, a "one-to-many" search compares a photograph or a live scan of someone's face to an existing database of thousands or millions of faces to attempt to find a match.[27] A police officer might use a one-to-many-search to narrow down a list of suspects by comparing a photograph or a sketch to a driver's license database. Other existing databases that could be used for such searches include mugshots, application photographs from immigrants applying for federal benefits, photographs of visa applicants, and photos taken at the United States border of people entering the country,[28] illustrating the range of circumstances that might circumstantially require someone to submit their photograph to a government database.

Understanding the different kinds of errors facial recognition systems can make is also key to understanding how they function. Both kinds of searches can result in false positives (the person identified is not truly the person the algorithm reported), or false negatives (the algorithm erroneously rejected the person whose face was scanned),[29] with varying implications depending on the context.

[23] *Hearing on Facial Recognition Technology*, *supra* note 13, at 17-18 (testimony of Meredith Whitaker, Co-Founder, AI Now Inst. NYU); LEARNED-MILLER ET AL., *supra* note 17, at 41.

[24] *Id*.

[25] *About Face ID Advanced Technology*, APPLE INC., https://support.apple.com/en-us/HT208108 [https://perma.cc/KZ9L-TFND]

[26] FACEPHI BEYOND BIOMETRICS, https://www.facephi.com/en/ [https://perma.cc/9XTP-8HM6].

[27] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019) [hereinafter NIST Study], https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/A3CD-K624] (describing the differences between one-to-one and one-to-many uses).

[28] These are the government databases NIST tested in a 2019 study of facial recognition algorithms. PATRICK GROTHER ET AL., NAT'L INST. OF STANDARDS AND TECH., NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT) (2019).

[29] NIST Study, *supra* note 27 ("A false positive means that the software wrongly considered photos of two different individuals to show the same person, while a false negative means the software failed to match two photos that, in fact, do show the same person.").

A false negative from an iPhone's face verification algorithm could lock someone out of their phone, and a false positive could let a stranger peruse its contents; a false negative from a one-to-many search conducted by law enforcement could mean that the true perpetrator evades suspicion, while a false positive could mean that someone innocent is erroneously made a suspect. Different uses produce different ramifications.

Furthermore, some algorithms are only designed to detect whether a face (or person) is present in the image, not to identify who the person is.[30] Facial recognition is one part of a broader set of capabilities that involve an algorithm assessing a face, such as gender, age, or ethnicity classification and affect classification, otherwise described as how a system attempts to assess the emotional state, attentiveness, or other cognitive attributes about the subject.[31] This article refers to "facial recognition technologies" as a class of technologies that include face detection, face identification, and affect analysis, and clarifies distinct capabilities where the additional specificity is needed.[32]

Commercial Uses of Facial Recognition Technologies

Private entities in a range of sectors are deploying facial recognition technologies to identify customers or authenticate their identity, as well as for a host of amorphous security uses. Retailers are using facial recognition to identify past or potential shoplifters.[33] Vendors like FaceFirst promote their wares with splashy taglines like "ready to reduce your in-store violence by up to 91%?"[34]

[30] *Id.*

[31] *Id.*

[32] My reasoning follows AI expert Meredith Whitaker's in her written testimony to the House Oversight Committee: "In this testimony I use the broad term "facial recognition" to include a range of technical capabilities, including face detection (recognizing a face in an image), facial identification and verification (recognizing a single face, and distinguishing it from others), and facial analysis (inferring demographics, identity, and interior traits based on face data). While these constitute discrete capabilities that are often treated separately within the AI research field, the deployment of these tasks raises shared concerns. These functions are also often linked or packaged together, as when facial analysis is sold as an "add-on" to facial recognition products. Furthermore, many systems for facial analysis are trained on the same datasets used to develop facial recognition and face-detection systems, meaning that bias and limitations from those datasets can affect performance on all tasks." *Hearing on Facial Recognition Technology*, *supra* note 13 (written testimony of Meredith Whitaker, Co-Founder, AI Now Inst. NYU).

[33] Chavie Lieber, *Your Favorite Stores Could Be Tracking You With Facial Recognition,* RACKED (May 22, 2018), https://www.racked.com/2018/5/22/17380410/facial-recognition-technology-retail [https://perma.cc/5QRS-NPYP].

[34] Description of Facial Recognition Services for Retail Stores, FACEFIRST (last visited June 22, 2020), https://www.facefirst.com/industry/retail-face-recognition/ [https://perma.cc/LSB8-DJRT]; *Sentinel-IQ Face Recognition Platform*, FACEFIRST (last visited June 22, 2020), https://www.facefirst.com/solutions/surveillance-face-recognition/ [https://perma.cc/D82X-SMRF].

and promises to "prevent retail crime" by comparing shoppers' images against "vast databases of criminals."[35] FaceFirst refused to reveal its clients, but stores like Walmart, Macy's, Lowes,[36] and Saks Fifth Avenue[37] have reportedly deployed facial recognition systems in their stores at various points in time, and the use of facial recognition in the retail sector remains widespread. Drugstores and grocery stores[38] are also deploying facial recognition systems along with shopping malls and boutiques. Vendors may set up sharing programs between stores, so that a shopper flagged by one store might be flagged in another they've never frequented before.[39] Casinos,[40] concert venues,[41] restaurants,[42] hotels,[43] and sports arenas[44] are also adopting facial recognition systems, out of a desire

[35] *Id.*; *Face Recognition for Retail Stores*, FACEFIRST, https://www.facefirst.com/industry/retail-face-recognition/ [https://perma.cc/Y3T9-M29T].

[36] Lieber*, supra* note 33.

[37] Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, N.Y. MAG. (Oct. 20, 2018), http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html [https://perma.cc/26XH-7AY4].

[38] *See* Tom Chives, *Facial Recognition… Coming to a Supermarket Near You*, THE GUARDIAN (Aug. 4, 2019), https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties [https://perma.cc/B8HU-2RHT]; *see generally* Description of Facial Recognition Services for Retail Stores, *supra* note 35.

[39] Alfred Ng, *With Facial Recognition, Shoplifting May Get You Banned In Places You've Never Been,* CNET (Mar. 20, 2019), https://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/ [https://perma.cc/WA5U-UXNG].

[40] *See* Jacob Solis, *How AI and Facial Recognition Could Reshape Las Vegas Casinos*, THE NEV. INDEP. (Jan. 21, 2020, 2:00 AM), https://thenevadaindependent.com/article/how-new-ai-and-facial-recognition-tech-could-reshape-las-vegas-casinos [https://perma.cc/ZGN2-HYHJ].

[41] *See* Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html [https://perma.cc/Z89X-EZQ2]. *But see* Matt O'Brien, *Concert Promoters Turn away From Facial Recognition Tech*, AP NEWS (Oct. 29, 2019), https://apnews.com/50be4fe7e9e644b897fb9d33ac11cea3 [https://perma.cc/4GF6-3Y73].

[42] *See* Kate Bernot, *Restaurants are Using Facial Recognition Software to Remember How You Like Your Burger,* THE TAKEOUT (June 29, 2018), https://thetakeout.com/restaurants-are-using-facial-recognition-software-to-re-1827237920 [https://perma.cc/U3VN-4G7P].

[43] NEC, https://www.nec.com/en/global/solutions/hospitality/security_face/index.html [https://perma.cc/ZPT9-UBNP].

[44] *See* Ryan Rodenberg, *Sports Betting and Big Brother: Rise of Facial Recognition Cameras,* ESPN (Oct. 3, 2018), https://www.espn.com/chalk/story/_/id/24884024/why-use-facial-recognition-cameras-sporting-events-the-rise [https://perma.cc/56LV-GTRX]; Niraj Chokshi, *Facial Controversies, From Stadium Surveillance to Racist Software,* N.Y. TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html [https://perma.cc/T3JB-KU6T].

to spot high-paying customers, make providing their service more efficient, or to identify "persons of interest." Hospitals are using facial recognition systems to verify patients,[45] landlords to verify tenants,[46] and airlines to verify passengers.[47] Systems that attempt to infer intent or ability from external emotional expressions are being tested in schools, used in hiring tools, and deployed with real-time surveillance systems, such as a program intended to predict likely shoplifters.[48]

The range of establishments deploying facial recognition systems is enormous, and they often don't clearly disclose their use of the technology.[49] In other cases, opting out may be impracticable or impossible,[50] or the location is one that cannot be avoided, such as a hospital or an airport. Unscrupulous image collection practices make it even more difficult to avoid having your face wind up in a database, as companies and researchers are scraping photographs from sources like Twitter and Facebook.[51] IBM, for example, released a diverse dataset intended for public use but built the dataset in part with pictures taken from

[45] FACE-SIX, https://www.face-six.com/patient-identification/ [https://perma.cc/PZP4-HUCE].

[46] *See* Erin Durkin, *New York Tenants Fight as Landlords Embrace Facial Recognition Cameras*, THE GUARDIAN (May 30, 2019), https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex [https://perma.cc/4HRC-6UDY]; Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. TIMES (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html [https://perma.cc/6MZA-R497]; Megan Wollerton, *Elecpro's Smart Lock Scans Faces to Let People In*, CNET (Jan. 8, 2019), https://www.cnet.com/news/elecpros-smart-lock-scans-faces-to-let-people-in-ces-2019/ [https://perma.cc/62JL-BDXG].

[47] Brown, *supra* note 16.

[48] *"Artificial Intelligence: Social and Ethical Implications": Hearing Before the H. Comm. On Science, Space and Tech.,* 116th Cong. 2-4 (2019) (written testimony of Meredith Whittaker, Co-founder and Co-director, AI Now Inst. NYU).

[49] GARVIE ET AL., *supra* note 17, at 58-60 (criticizing the lack of transparency surrounding law enforcement uses of facial recognition technology); *Facial Recognition Technology (Part I): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight and Reform,* 116th Cong. 2 (2019) [hereinafter *Hearings*] (written testimony of Joy Buolamwini, Founder, Algorithmic Justice League) (describing the ubiquity of facial recognition surveillance and the lack of transparency concerning its use).

[50] Allie Funk, *I Opted Out of Facial Recognition at the Airport—It Wasn't Easy*, WIRED (July 2, 2019), https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/ [https://perma.cc/XM4W-CTAW].

[51] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/6MKE-66R5].

the photo-sharing site Flickr without the subjects' consent.[52] Until NBC News reported on the state of affairs and built an accompanying search tool, there was no way for Flickr users to determine if their photographs had even been used, knowledge they would have to have in order to opt out of those uses.[53]

Government Uses of Facial Recognition Technologies

Government uses of facial recognition technologies are often even more coercive and surreptitious than commercial ones, and often have more severe implications due to the authority the governmental entity might have, and the context in which the technology is used. Some cities, like Detroit, have attempted to deploy facial-recognition cameras widely specifically to "deter crime,"[54] including in public housing.[55] Simply walking around in Detroit, or being in an economic circumstance that requires you to rely on public housing, could be enough for your face to wind up in a database, available for perusal by the police.[56] The use of facial recognition by police departments has spread rapidly, with one estimate placing the facial recognition market for federal, state and local law enforcement at $375 million by 2025, up from $136.9 million in 2018.[57] A landmark report by the Center on Privacy & Technology at Georgetown Law in 2016 placed its "conservative" estimate for how many police departments were using facial recognition at *one in four.*[58] Law enforcement agencies use them for both investigation and surveillance, including searching

[52] Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 12, 2019), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/YU4F-2KTA].

[53] *Id.*

[54] Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer [https://perma.cc/9V77-UHLE]

[55] Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html [https://perma.cc/P3XZ-7TYU].

[56] Clare Garvię & Laura Moy, *Face Surveillance in the United States,* AMERICA UNDER WATCH (May 16, 2019), https://www.americaunderwatch.com/ [https://perma.cc/3XU4-LPYN].

[57] Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/B75T-QEWG].

[58] *See id.*; GARVIE ET AL., *supra* note 17, at 3; Drew Harwell, *Both Democrats and Republicans Blast Facial-Recognition Technology in a Rare Bipartisan Moment,* WASH. POST (May 22, 2019), https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control/.

video footage, monitoring or tracking people in real time, track specific individuals in real time, and attempting to identify suspects.[59]

State and local police departments also aren't the only government agencies relying on facial recognition. Federal agencies like Immigrations and Customs Enforcement have searched for immigrants to deport using state drivers' license databases, including states that permit immigrants to obtain those licenses regardless of immigration documentation.[60] The Government Accountability Office reported in 2019 that 21 states and the District of Columbia allow federal agents to scan their driver's license databases, and the FBI[61] collectively has access to more than 641 million face photographs across a range of government databases.[62]

Child-Specific Uses of Facial Recognition Technologies

Young people experience many of the uses of facial recognition that adults are subjected to, such as companies scraping photographs from social media to build facial recognition databases, or using the technology on photos that users upload. They also experience real-time surveillance, such as the systems used to monitor large spaces like a shopping mall, and anywhere else the technology is deployed where children might happen to be, whether alone or accompanied by an adult. Children and teenagers with iPhones might use the device's facial recognition verification systems to unlock their phones;[63] teenagers with bank accounts might use a mobile banking application's facial recognition verification system. In 2019, the Georgetown Center on Privacy & Technology found that the New York Police Department had been comparing crime scene images to databases of juvenile mugshots, some taken from children as young as 11

[59] *See* Ferguson, *supra* note 18, at 9-15.

[60] Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/HHN8-FVBS]; Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/64HM-TGX9].

[61] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS 3-4 (2019) (statement of Gretta L. Goodwin, Director, Dep't. of Homeland Security and Justice).

[62] Harwell, *supra* note 60; *Facial Recognition Technology Hearings, supra* note 49, at 6 (statement of Neema Singh Guliani, Senior Legis. Couns., ACLU).

[63] Victoria Rideout & Michael Robb, *The Common Sense Census: Media Use by Tweens and Teens*, COMMON SENSE MEDIA (2019), https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-census-8-to-18-keyfindings-updated.pdf [https://perma.cc/D7JE-8RKP] (citing statistics about general smartphone use by children and teenagers).

years old, for four years.[64] General uses of facial recognition systems might supplement child-specific uses, such as the watch list scanned by the Texas City school system's facial recognition technology, which was supplemented with pictures from social media and Ring doorbell cameras.[65]

But children are also subjected to uses of facial recognition technology that are specific to them. The use of facial recognition systems in schools has become more prevalent as the technology has grown cheaper, and concerns about gun violence drive schools to seek whatever solutions available to them to keep children safe, including surveilling the students they're trying to protect.[66] While the wisdom of turning to surveillance to combat a surfeit of guns is misguided, the existence of the surveillance remains. The service that the Lockport, New York school system attempted to implement, for example, would have enabled school officials to track students' movements around campus after their picture had been uploaded to the database.[67] Proponents argued that being able to recognize anyone who isn't permitted to be on school property will keep students safer,[68] without grappling with the impact to the students' privacy, free expression, and intellectual development of constant surveillance, nor the implications for students of color whom the technology may wrongly identify. Face-Six, the Israeli facial recognition company that supplied an after-school center in Bloomington, Indiana, with its facial recognition system, promotes the same system for use in prisons;[69] AnyVision, the Israeli company that sold a facial recognition system

[64] Goldstein & Watkins, *supra* note 8.

[65] Tom Simonite & Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, WIRED (Oct. 17, 2019), https://www.wired.com/story/delicate-ethics-facial-recognition-schools [https://perma.cc/6NC2-E6C6].

[66] Drew Harwell, *Unproven Facial-Recognition Companies Target Schools, Promising an End to Shootings*, WASH. POST (June 7, 2018), https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html [https://perma.cc/YL56-FQ2J] (discussing the rise and prevalence of school surveillance, particularly social media monitoring, "as an all-seeing shield against school shootings"); Faiza Patel et al., *School Surveillance Zone*, BRENNAN CENTER FOR JUSTICE (Apr. 30, 2019), https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone [https://perma.cc/PS3S-D2MW] ("A number of companies, many of which have sprung up in the last five years, are selling software that can allegedly identify signs of violence or other concerning behavior by trawling children's social media posts and other online activity."); Vaidya Gullapalli, *New to the School-to-Prison Pipeline: Armed Teachers, Facial Recognition, and First-Graders Labeled 'High-Level' Threats*, THE APPEAL (Oct. 21, 2019), https://theappeal.org/new-to-the-school-to-prison-pipeline-armed-teachers-facial-recognition-and-first-graders-labeled-high-level-threats/ [https://perma.cc/8DEC-D7MM].

[67] Letter from John A. Curr III, Western Regional Office Director, NYCLU, to Mary Ellen Elia, Comm'r, N.Y. State Educ. Dept. (June 18, 2018) (on file with the NYCLU).

[68] Simonite & Barber, *supra* note 65 ("It's a very, very efficient way of monitoring a group of people" says the IT director for the Putnam City, Oklahoma school district).

[69] Harwell, *supra* note 66.

to the Putnam City and Texas City school districts, has also supplied the Israeli army with the technology to be used at army checkpoints in the West Bank.[70]

Other child-centric organizations have implemented facial recognition systems out of a desire to protect children by surveilling them. Summer camps have begun to use facial recognition systems as well, both for intended safety reasons and to provide parents with pictures of their children.[71] A company called FaceFirst offers customers the capability to "capture photographs of potential victims" of kidnapping and human trafficking, specifically children, "from a safe distance,"[72] and claims to be able to prevent bias based on age, race and gender.[73] While the company's intentions are likely good, the implications of selling a facial recognition product that people can point at strange children are dangerous for the privacy and safety of those children, particularly given the risk of overanxious intervenors wrongly suspecting children in mixed-race families.[74] Another company, Clearview AI, has reportedly been used to identify pictures of underage victims of sex trafficking on social media.[75]

In some cases, a child's own parents might be surveilling them. Closeli nanny cams, for example, include by facial-recognition capabilities.[76] In a world where people of all ages cannot easily escape facial surveillance, children are often subjected both to general-purpose uses of these technologies, and child-specific forms out of misguided attempts to keep them safe.

FACIAL RECOGNITION'S HARMS

Facial recognition systems are being deployed across the gamut of possible sectors, and on all kinds of people. The ubiquity of these technologies makes the

[70] Simonite & Barber, *supra* note 65.

[71] Drew Harwell, *As Summer Camps Turn on Facial Recognition, Parents Demand: More Smiles, Please*, WASH. POST (Aug. 8, 2019, 4:26 PM), https://www.washingtonpost.com/technology/2019/08/08/summer-camps-turn-facial-recognition-parents-demand-more-smiles-please/ [perma.cc/Q2TW-XLDV].

[72] *Find Missing Children with Face Recognition*, FACEFIRST, https://www.facefirst.com/industry/missing-children/ [https://perma.cc/2X6V-4G3V].

[73] *Our Commitment to Personal Privacy*, FACEFIRST, https://www.facefirst.com/privacy-commitment/ [https://perma.cc/CNW7-LF9X].

[74] Jonathan J. Cooper, *Strangers' Suspicions Rankle Parents of Mixed-Race Children*, AP NEWS (Feb. 13, 2019), https://apnews.com/9e73ee4106c74188b643f91c7ed59157 [perma.cc/2PLN-F7RL].

[75] Hill & Dance, *supra* note 3.

[76] *What's Closeli?*, CLOSELI, https://www.closeli.com/ [https://perma.cc/GZP3-PMN8]. It is also worth noting that in the case of this particular company, Closeli explicitly markets their camera for use on children, as demonstrated by the home page that suggests the product may be used "by Mom and Dad" to record children after they come home from school, and note that the product offers "optional facial tracking" so that the product "[k]nows the difference between your kids and that car in the background." Yet, its privacy policy claims that the company "will not *knowingly* collect personal information from children under 18" (emphasis added), which seems improbable at best.

threats they pose to privacy, free expression, safety, and fundamental fairness similarly ubiquitous. Facial recognition technologies have concerning implications given their lack of accuracy for certain demographic groups, including children, and the particularly severe consequences that the privacy invasions they inflict will have on vulnerable young people. But the harms that facial recognition technologies enable are not unique to the populations for whom those technologies are inaccurate—the erosion of practical obscurity and cheap surveillance of scores of people threatens freedom for everyone.

To demonstrate how facial recognition's harms are distributed and why a comprehensive ban is preferable to a child-specific ban, I've distinguished quasi-universal harms, shared harms, and child-specific harms. These categories are overly simplistic, but useful for illustrating the value of a comprehensive ban, and why a child-specific ban is neither sufficient nor coherently defensible. I refer to broadly applicable harms as "quasi-universal" because unlike errors tied to an immutable characteristic, these are harms are theoretically capable of being experienced by anyone (though in practice they are disproportionately dispersed among certain groups, particularly people of color, women of color, and the poor). Shared harms are the harms that are felt by demographic groups in addition to children, but not capable of being universally experienced due to being tied to immutable characteristics apart from youth that the entire population does not share, such as race and gender. Child-specific harms are not unique to them, but may be uniquely severe in some ways for them due to their developmental vulnerabilities and the disproportionate effects that experiencing facial recognition's harms early in their lives may have.

Quasi-Universal Harms

Facial recognition's most dangerous attribute—that it enables unavoidable, dragnet surveillance of law-abiding activity on a massive scale—helps explain why its harms to privacy, free expression, and due process are so broadly felt. As one example, more than 227 million Americans held driver's licenses in 2019,[77] and at least 26 states permit law enforcement to run facial recognition searches on those databases.[78] The landmark Georgetown report estimated in 2016 that as many as one in two Americans have had their photos searched in that way.[79] As both cameras and facial recognition technologies grow cheaper and more advanced, more institutions have begun to implement various forms of the technology, the surveillance becomes harder to escape. If you have a drivers' license, walk around a public place monitored by cameras, or use social media, your face is most likely in a facial recognition database (with or without your knowledge).

[77] *How Many Licensed Drivers Are There In The US?*, HEDGES & COMPANY, https://hedgescompany.com/blog/2018/10/number-of-licensed-drivers-usa/ [https://perma.cc/DMA6-Y6E7].

[78] GARVIE ET. AL., *supra* note 17, at 2.

[79] *Id.*

Other privacy risks are similar to those created by other biometrics, such as fingerprints, palm prints, or irises, but are still not quite as severe as the implications of facial recognition. Photographs are used far more widely for identification, allowing the creation of databases from photographs collected for different purposes. As one example, no one is posting pictures of their palm prints on Facebook—they're posting pictures of their faces. Facial recognition can be used to quickly review faces in large crowds in a way that iris recognition, palm-print recognition, and fingerprint recognition cannot be.[80]

Facial recognition technologies are particularly corrosive of practical obscurity, the effect of realistic constraints such as cost, feasibility, volume, and even the fallibility of human memory on the functional availability, and thus privacy implications, of ostensibly available information.[81] Facial recognition searches and surveillance erode the barriers of practical obscurity by enabling the searcher or watcher to connect a physical face to a name and list of facts about the subject, and then combine photographic databases that were compiled under different circumstances. Woodrow Hartzog and Evan Selinger have written extensively about how facial recognition's threat to practical obscurity makes it a uniquely dangerous surveillance technology,[82] and as they point out,[83] the invasions that facial recognition technologies enable make the previous assumptions one could make about privacy in public obsolete. The risk assumed by simply venturing into the public square is categorically different when law enforcement is able to cheaply, quickly, and quietly identify you on the spot, even when you have had no previous contact with law enforcement whatsoever.

[80] Your irises, like your face, do not change meaningfully over the course of your life, except in the case of some diseases; but among other things, it is far easier to hide your eyes in a crowd than it is to hide your entire face. GARVIE ET AL., *supra* note 17, at 10; Adam Czajka et al., *How to Teach an Iris Scanner That the Eye It's Looking at Is Dead*, IEEE SPECTRUM (Aug. 29, 2019, 3:00 PM), https://spectrum.ieee.org/biomedical/imaging/how-to-teach-an-iris-scanner-that-the-eye-its-looking-at-is-dead [https://perma.cc/GDR4-7HVP].

[81] *See* Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy, in* ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY 1, 2 (Joseph Pitt & Ashley Shew eds. 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866 [https://perma.cc/N5CE-A55S] ("Obscurity is the idea that information is safe—at least to some degree—when it is hard to obtain or understand . . . When information is hard to understand, the only people who will grasp it are those with sufficient motivation to push past the layer of opacity protecting it.").

[82] *Id.* at 3; *See also* Woodrow Hartzog & Frederic Stutzman, *Obscurity By Design*, 88 WASH. L. REV. 385, 406 (2013), https://cyberlaw.stanford.edu/files/publication/files/ssrn-id2284583.pdf [https://perma.cc/X2W7-TDGL]; Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 459 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084102 [https://perma.cc/BW2K-BBQS]; Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in The Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html [https://perma.cc/8CQC-KQHB].

[83] Selinger & Hartzog, *supra* note 81, at 4; Hartzog, *supra* note 82, at 469.

By relying on photos taken in a range of circumstances, facial recognition systems collapse contextual distinctions that are a crucial component of privacy.[84] Law enforcement systems run comparison searches on mugshot photos (meaning that the subject may not have been convicted of a crime), photos from drivers' licenses, and photos from social media, while the algorithms they're relying on have likely been trained on pictures obtained without the subjects' consent. Simply put, photographs are collected and disseminated for all kinds of reasons that may implicate very different parts of a person's life.

This context collapse is only likely to accelerate. The race to improve facial recognition algorithms by training them on larger and more diverse datasets has incentivized researchers and companies to obtain as many useable photographs as they can through whatever means they can.[85] One notorious company, Clearview AI, enables users to take a picture of someone, upload it, and quickly access publicly available photos of that person scraped from millions of websites, along with links to where those pictures were originally found.[86] As facial recognition technologies become even cheaper and easier to use, and the social norms around their use continue to evolve, the boundaries between how the pictures were made available and how researchers, companies, and the government will use them will only crumble faster.

Attempts to infer personal attributes or emotions from someone's facial expression also invite privacy invasions and discrimination.[87] The long and ugly history of pseudoscientific attempts to connect physical appearance to mental and moral aptitude will not be improved or corrected by incorporating those methods into algorithms. Systems that promise to "assess criminality" or assess a job applicant's candidacy for the position will only reify existing inequality by providing a supposedly scientific justification for discrimination.[88] Studies have found that not only are the claims made by the companies selling emotional analysis products unsupported,[89] but that these systems introduce an additional form of racial bias by misinterpreting the facial expressions of Black people,[90] generally providing them with more negative scores on average than people of other ethnicities. As fairness in machine learning expert Meredith Whitaker

[84] *See* Selinger & Hartzog, *supra* note 81, at 3-4.

[85] Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 17, 2019), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/4T2K-LLYV].

[86] Hill, *supra* note 51.

[87] Brown, *supra* note 16.

[88] SARAH MYERS WEST ET AL., DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI 3 (AI Now Institute ed. 2019).

[89] Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 PSYCHOL. SCI. IN THE PUB. INT., 1, 47-48 (2019).

[90] Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions* 6 (Nov. 9, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.

noted in testimony before the House of Representatives, emotional analysis technologies are being deployed in all sorts of contexts where erroneous assessments could limit the life opportunities and well-being of the subject, from assessing job candidates, to attempting to gauge a patient's pain, discerning which shoppers are most likely to shoplift, determining which students in a classroom are paying attention, or assessing someone's sexuality.[91]

Facial recognition technologies also threaten free expression. As Neil Richards has written about at length, intellectual privacy is a necessary condition for the exercise of the mental autonomy that free expression protections are intended to facilitate.[92] Without the ability to think, write, and communicate in private, we self-censor and choose not to experiment with ideas that risk eliciting social, legal, or physical consequences.[93] As Richards puts it, "surveillance inclines us to the mainstream and the boring."[94]

The knowledge that law enforcement is capable of quickly and cheaply identifying people in a crowd can deter political protest, as people may be correctly afraid of reprisals. People may be concerned about having their photos collected and used to identify them in real life, which may prevent them from using social media to connect with family, friends, readers, audiences for products they create, and others. The inability to preserve anonymity in public and on the internet corrodes the ability of anyone afraid of having their identity used against them to speak freely.[95]

Nor are such fears irrational. In the 2016 Georgetown report examining how facial recognition technologies are used by law enforcement, only one of the fifty-two law enforcement agencies they examined had a use policy that expressly prohibited officers from using them to track people engaged in "political, religious, or other protected speech."[96] In 2016, the ACLU of Northern Califor-

[91] *Hearing on Facial Recognition Technology*, *supra* note 13, at 14 (testimony of Meredith Whitaker, Co-Founder, AI Now Inst. NYU);. 14 (2020); Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images*, 114 J. OF PERSONALITY AND SOC. PSYCHOL. 246, 254-56 (2018).

[92] Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 388-391 (2008) ("At the core of the First Amendment is a commitment to the freedom of thought— recognized for centuries as the most vital of our liberties. In order to speak, it is necessary to have something to say, and the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants. . . . If we are interested in a free and robust public debate we must safeguard its wellspring of private intellectual activity.")

[93] Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) ("With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.").

[94] *Id.* at 1948.

[95] *See id.* at 1949.

[96] GARVIE ET. AL. *supra* note 17, at 3.

nia found that the Baltimore Police Department used facial recognition to identify protestors in real time,[97] and in 2018, the Secret Service also began testing a facial recognition system in the public areas around the White House in order to help it identify "known subjects of interest."[98] More recently, police in Delhi used facial recognition software to screen crowds at a rally for Prime Minister Modi;[99] in Hong Kong, law enforcement authorities have access to facial recognition technology that can identify protestors,[100] many of whom took to covering their faces for that very reason.[101] Surveillance of political protestors is a shameful tradition that is no less harmful via digital methods than it is through analog ones.[102] The threats that facial recognition poses to the democratic rights of free assembly, expression, and political dissent are concrete, severe, and broadly applicable.

Facial recognition technologies also threaten components of due process that are fundamental to how the American criminal justice system is intended to work.[103] Simply by having a driver's license, Americans could be included in a law enforcement database that an officer or agent could use to search for possible

[97] Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Tool was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016) https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api [https://perma.cc/HHW9-JNYS].

[98] Jay Stanley, *Secret Service Announces Test of Face Recognition System Around White House*, ACLU (Dec. 4, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-service-announces-test-face-recognition [https://perma.cc/F4YY-ERHB]; U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FACIAL RECOGNITION PILOT, DHS/USSS/PIA-024 at 2 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf.

[99] Chandran, *supra* note 7.

[100] Blake Schmidt, *Hong Kong Police Already Have AI Tech That Can Recognize Faces*, BLOOMBERG (Oct. 22, 2019), https://www.bloomberg.com/news/articles/2019-10-22/hong-kong-police-already-have-ai-tech-that-can-recognize-faces [https://perma.cc/YZ6T-E665].

[101] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N.Y. TIMES (July 26, 2019), https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html [https://perma.cc/EGD9-FSYZ].

[102] *See* GARVIE ET. AL., *supra* note 17, at 41 (discussing the FBI's surveillance of Martin Luther King Jr., Fannie Lou Hamer, Cesar Chavez and other civil rights leaders); Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ [https://perma.cc/ECT7-YBDU] ("As with the scientific racism of old, facial recognition doesn't simply identify threats; it creates them, and as such intensifies a dangerous digital moment with a long history.")

[103] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/U455-WV9F] (discussing Florida police departments' reliance on facial recognition systems and how system errors create due process concerns).

suspects of a crime.[104] The possibility that anyone may be subject to suspicion invites what can accurately, if somewhat dramatically, be described as tyranny: individualized suspicion is a key law enforcement constraint and pillar of our criminal justice system, and it is undermined by technology that, in the words of the Georgetown experts who conducted the landmark 2016 study, enrolls you in a "perpetual line-up."[105] A false positive can endanger someone's freedom or even their life—after facial recognition technology misidentified Muslim activist Amara K. Majeed as a suspect in the Sri Lanka Easter bombings, she received death threats and her family members in Sri Lanka were harassed by the police, even after the FBI put out a public statement correcting its mistake.[106] The South Wales police department stored the records of 2,297 people after misidentifying them, reporting a jaw-dropping false positive rate of 92%.[107]

The use of facial recognition systems by law enforcement is also subject to little oversight or quality control.[108] Law enforcement officials often do not confine themselves to using only the high-quality images that facial recognition algorithms are designed to identify. A recent report by the Georgetown Center on Privacy & Technology found that at least a half-dozen police departments across the country are comparing forensic sketches to facial recognition databases when the officers don't have a photograph of the suspect, despite the fact that sketches are of far too low a quality to provide an accurate result.[109] The report also found that police departments have used photos of celebrities, or edited the photos of suspect photographs, adding additional potential for error and arbitrary results.[110]

Human review is a common and popular proposed check on algorithmic decision-making systems, the idea being that if the machine's assessment is always tempered by a human being's corrective analysis, the human being should be able to catch the machine's mistakes. But automation bias, the tendency of human beings to trust the judgment of computers over their own without a rational basis to do so, makes this a less effective check that facial recognition defenders tend to claim.[111]

Furthermore, while police departments often claim that facial recognition searches are never relied upon as determinative evidence for an arrest, those

[104] *See id.*

[105] *See generally* GARVIE ET. AL., *supra* note 17.

[106] *Facial Recognition Technology Hearings, supra* note 49, at 7 (testimony of Joy Buolamwini, Founder, Algorithmic Justice League).

[107] Cyrus Farivar, *UK Police Say 92% False Positive Facial Recognition Is No Big Deal,* ARS TECHNICA (May 7, 2018 2:26 PM), https://arstechnica.com/tech-policy/2018/05/uk-police-say-92-percent-false-positive-facial-recognition-is-no-big-deal/ [https://perma.cc/PFH3-96V4].

[108] Garvie, *supra* note 21.

[109] *Id.*

[110] *Id.*

[111] *Id.* (defining automation bias).

claims seem dubious. In Detroit, Julian-Borchak Williams was wrongfully arrested for larceny that he did not commit, based on his erroneous identification by a facial recognition algorithm—the first known case of its kind.[112] While Mr. Williams' case is the first known example of facial recognition technology being the direct basis for a wrongful arrest, it is highly unlikely to be the only example that exists. After Mr. Williams' story was reported by the New York Times, the Detroit police chief described the facial recognition system his department has relied on as misidentifying suspects "96% of the time."[113] In Florida, for example, the New York Times found that in a few cases where officers used facial recognition to locate a suspect, documents indicated that there was no other evidence.[114] State laws vary as to what methods and materials law enforcement are required to disclose to the defendant, and states often refuse to disclose their use of facial recognition, instead referring vaguely to facial recognition searches as "investigative means" or "attempt[s] to identify."[115] In New York, the attorneys for a man arrested for theft argued that there was no probable cause to arrest their client beyond the facial recognition search that NYPD officers ran of an image of their client, only months after NYPD Commissioner wrote in the New York Times that a match would never be used as the sole basis for arrest.[116] The Bronx DA's office claimed that the match was not the sole basis for the probable cause to arrest, and also argued that it was not required to disclose information about how the technology had been used.[117] On the day of the trial, the office lowered the charges from a felony to a misdemeanor with time served, which an observer might conclude was related to concerns that a judge might agree with the defense's arguments and the NYPD's use of facial recognition could be subjected to unwanted scrutiny.[118] This would not be an implausible tactic, as it has previously been deployed by prosecutors' offices to obscure their reliance on cell-site simulators.[119]

[112] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/4DCL-HBW2].

[113] Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, VICE (June 29, 2020, 12:56 PM), https://www.vice.com/en_us/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time [https://perma.cc/8YJR-5AHH].

[114] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition and Where It Falls Short*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/LVD6-8Y5S].

[115] *Id.*

[116] Mike Hayes, *Is This the Guy?*, THE APPEAL (Aug. 20, 2019), https://theappeal.org/is-this-the-guy/ [https://perma.cc/U4WY-Z3JK].

[117] *Id.*

[118] *Id.*

[119] Cyrus Farivar, *FBI Would Rather Prosecutors Drop Cases Than Expose Stingray Details*, ARS TECHNICA (Apr. 7, 2015), https://arstechnica.com/tech-policy/2015/04/fbi-would-rather-prosecutors-drop-cases-than-disclose-stingray-details/ [https://perma.cc/T3XZ-Z446].

The lack of transparency surrounding the use of facial recognition technologies by law enforcement makes the lack of standards and oversight all the more concerning for individual civil liberties. The 2016 Georgetown study, *Perpetual Line-Up*, found that only four of the fifty-two law enforcement agencies surveyed had any kind of publicly available policy concerning their use of facial recognition.[120] Law enforcement agencies are cagey about their use of this technology, admitting its existence, but providing limited information in response to public records requests. Facial recognition technology vendors like Amazon even use non-disclosure agreements with law enforcement to keep its use of the technology from the public.[121] Surveys of public defenders have also illustrated that prosecutors frequently fail to disclose necessary information about law enforcement use of facial recognition technologies,[122] which the ACLU has argued are often unconstitutional violations of defendants' *Brady* rights.[123] There are few quality controls or oversight mechanisms over law enforcement uses of facial recognition databases, meaning that errors may go undetected and uncorrected.[124]

The damage that facial recognition technologies inflict on privacy, free expression, and due process affects us all, and should not be taken lightly. Even if facial recognition technology weren't fraught with biased accuracy problems or deployed with sloppy haphazardness that raises the likelihood of errors, it would still pose a severe threat to democratic values working exactly as intended.

Shared Harms

Facial recognition technologies inflict what can be described as quasi-universal harms by virtue of the fact that they are a dragnet surveillance tool—anyone with a picture in a government database, who posts a picture on a commercial internet service, or ventures outside in public with their face uncovered is implicated. The term "universal" risks implying that the harms of facial recognition are equally dispersed when they are not—populations that were already more vulnerable to surveillance and over-policing are much more susceptible. I use it to distinguish the category of harms that, theoretically, could affect the vast majority of the population, from facial recognition's accuracy problems with different demographic groups, which are not universal in the same way.

Facial recognition technologies are all the more damaging because they do not perform with equal accuracy for different demographic groups. A range of studies show that facial recognition algorithms are less accurate for people with

[120] GARVIE ET AL., *supra* note 17, at 58.

[121] Davey Alba, *With No Laws to Guide It,* BUZZFEED (Oct. 30, 2018), https://www.buzzfeednews.com/article/daveyalba/amazon-facial-recognition-orlando-police-department [https://perma.cc/V28T-YT7E].

[122] *Facial Recognition Technology Hearings, supra* note 49, at 17 (statement of Clare Garvie, Senior Associate, Ctr. on Privacy and Tech. at Georgetown Law).

[123] *Id*. at 4 (statement of Neema Singh Guliani, Senior Legis. Couns., ACLU).

[124] GARVIE ET AL., *supra* note 17, at 46-7.

darker skin,[125] women,[126] transgender and non-binary individuals,[127] the elderly,[128] and (as will be discussed in the next section) children.[129] Facial recognition poses specific harms for each of the demographic groups for whom it performs poorly.

The life cycle of the development and use of a facial recognition system creates a number of junctures that researchers have posited could be responsible for inaccuracies based on race, gender, and age, including composition of the datasets of face images used to train facial recognition algorithms[130] and the composition of the datasets used as benchmarks.[131] A dataset that contains faces that are mostly white, middle-aged men will establish its criteria for how to evaluate faces according to the samples in that set, meaning that such an algorithm would likely be more accurate for those faces, and less so for others.[132] As an example, a recent National Institute of Standards and Technology (NIST) study that evaluated 189 algorithms from 99 different developers, the study found high rates of false positives of Asian, Black, and native faces relative to white faces among U.S.-developed algorithms, whereas algorithms developed in Asian countries showed no dramatic difference in accuracy for assessments of Asian faces and white faces.[133] While the researchers do not go so far as to claim a causal relationship, they do note that the disparity supports the idea that the diversity of the training data impacts the accuracy of the algorithm for the demographic groups it is used to identify.[134]

[125] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. ON MACH. LEARNING RES.: CONF. OF FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 1, 2-8 (Feb. 2018); Inioluwa Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, 2019 CONF. ON ARTIFICIAL INTELLIGENCE, ETHICS, AND SOC'Y 1- 5; Joy Buolamwini, *When the Robot Doesn't See Dark Skin,* N.Y. TIMES (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html_[https://perma.cc/CZ32-ERFJ].

[126] *See* Buolamwini & Gebru, *supra* note 125, at 6, 8, 10; Raji & Buolamwini, *supra* note 125, at 4; Buolamwini, *supra* note 125.

[127] Os Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, 2 PROC. OF THE ACM ON HUMAN-COMPUTER INTERACTION 1, 4 (2019).

[128] *See* GROTHER ET AL., *supra* note 28, at 2, 8, 17.

[129] *Id*. at 2.

[130] NIST, *supra* note 27.

[131] LEARNED-MILLER ET AL., *supra* note 23.

[132] *See* Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS AND SECURITY 1789, 1791 (Dec. 2012), https://bit.ly/2TGiWaO [https://perma.cc/GV93-2M7H]; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1 (2018), https://bit.ly/2Ek9ZwZ [https://perma.cc/839J-9SD2].

[133] NIST Study, *supra* note 27.

[134] *Id.*

In the case of law enforcement searches, this disparity makes those groups of people more vulnerable to erroneous identification and accusation of crimes they did not commit.[135] The 2019 NIST study found that the faces of Black women showed the highest rates of false positives in one-to-many matching—the kind of search a law enforcement official would use to attempt to identify a shortlist of suspects.[136] In one such case, a man in Florida named Willie Lynch is appealing an eight-year prison sentence after the Jacksonville Sherriff's Office identified him using facial recognition, despite the fact that he was never permitted to see the four other "possible matches" that the system identified.[137] Lynch is Black, supporting the likelihood that the system erroneously identified him—the system only reported a likelihood of "one star" that the assessment was correct, and the analyst running the test was not even aware of how many "stars" were available.[138] Mr. Williams, the man wrongfully arrested on larceny charges due to erroneous identification by the Detroit Police Department's facial recognition system, is also Black.[139]

The opaque use of facial recognition systems that misidentify people of color exacerbates other forms of structural racism in the criminal justice system. Black people are already the disproportionate targets and victims of unjust policing practices that endanger their lives and liberty more than other demographic groups, and the risks these technologies pose to their freedom, and to the function of a fair criminal justice system, are neither remote nor abstract.[140] Over-policing of communities of color means that facial recognition technology is more likely to be used against them as surveillance or investigative tool.[141] The 2019 NIST study also reported that Native American faces had the highest rate of false positives,[142] putting them at similar risk— like Black people, Native Americans are incarcerated and killed by law enforcement at far higher rates than other demographic groups.[143] The opaque use of a surveillance technology

[135] *See* Garvie, *supra* note 21, at 18-19 (discussing Lynch case).

[136] NIST Study, *supra* note 27.

[137] *Facial Recognition Technology Hearings, supra* note 49, at 18 (statement of Clare Garvie); Somil Trivedi & Nathan Freed Wessler, *Florida is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech*, ACLU (Mar. 12, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people [https://perma.cc/7RPH-TC5S].

[138] Brief for American Civil Liberties Union et al. as Amici Curiae Supporting Petitioner at 3, Lynch v. State of Florida, No. SC2019-0298 (Fla. 2019).

[139] Hill, *supra* note 112.

[140] *Facial Recognition Technology Hearings, supra* note 49, at 5 (statement of Neema Singh Guliani).

[141] *Id.*

[142] NIST Study, *supra* note 27.

[143] *See Incarceration Rates for Native Americans*, NATIVE AMERICA: A HISTORY (Mar. 9, 2018), https://michaelleroyoberg.com/current-events/incarceration-rates-for-native-americans/ [https://perma.cc/H8XS-ZUX8]; Mike Males, *Who Are Police Killing?,* CTR. ON

that has a higher chance of misidentifying them exacerbates these racist and undemocratic structural failures. Everyone is hypothetically subject to the criminal justice system and capable of experiencing the kinds of arbitrariness and unfairness that facial recognition systems can inject—but in reality, these harms will not be dispersed equally among demographic groups.

Gender-based inaccuracies also have disturbing implications for the use of facial recognition technologies. NIST's most recent study found that false-positives were between two to five times more likely for women than men, with a range across the particular algorithm tested, and the country of origin and age of the subject.[144] The study found particularly high failed match rates in the mugshots of Asian and Black women,[145] similarly putting then at risk of wrongful identification in a law enforcement search, or a search conducted by a private company for security purposes.

Inaccurate results, including higher false positive rates for women than men, are one issue. Another is flawed gender classification algorithms, namely when an algorithm is designed to assess a person's gender by analyzing facial geometry or other metrics like skin texture.[146] They are often not created to assess any option beyond the male-female binary.[147] As an example, in the December 2019 NIST test of false match rates for certain age groups, researchers discarded the images for which sex was not listed as male or female,[148] and none of the tests include a sex option beyond male or female. As Os Keyes explains in their research on automated gender recognition, most facial recognition systems that assess the gender of the subject operationalize a binary conception of gender, and ignore the existence of transgender or non-binary people entirely.[149] This, too, can have discriminatory effects: some transgender Uber drivers have been unable to drive for the company when the app's verification mechanism incorrectly failed to verify their identity.[150] Incorrect assessments of someone's gender could have inconvenient, discriminatory or dangerous implications for the subject, depending on the context. The erasure of transgender identity by coding a refusal to acknowledge it into facial recognition systems is dehumanizing and

JUVENILE AND CRIMINAL JUSTICE (Aug. 26, 2014), http://www.cjcj.org/news/8113 [https://perma.cc/S7SN-M3NU].

[144] GROTHER ET AL., *supra* note 28, at 7.

[145] *Id.* at 47.

[146] Keyes, *supra* note 127*,* at 88:4.

[147] *Id.* at 88:1.

[148] GROTHER ET AL., *supra* note 28, at 49.

[149] Keyes, *supra* note 127, at 88:1-2.

[150] Jaden Urbi, *Some Transgender Drivers Are Being Kicked Off Uber's App*, CNBC (Aug. 8, 2018, 11:16 AM), https://www.cnbc.com/2018/08/08/transgender-uber-driver-suspended-tech-oversight-facial-recognition.html [https://perma.cc/3GRC-WCPN].

regressive for the transgender and non-binary people whose identities the system ignores.[151]

The discriminatory effects of commercial uses of facial recognition and analysis are still alarming, even when they do not immediately threaten the subject's safety. Consider HireVue, the company that offers a job candidate screening service that employs facial analysis technology to assess actions and attributes like "vocal indications of enthusiasm," facial expression and eye contact from job applicants.[152] Aside from the fact that the service's claims of being able to deduce enthusiasm and aptitude from facial expression, eye contact, and similar attributes is worrisomely reminiscent of 19th century physiognomy, an algorithm that cannot assess a given demographic group accurately puts candidates who belong to those groups at risk of being misinterpreted and unwittingly discriminated against in the hiring process.[153] Certain commercial uses, such as surveillance of retail spaces to identify people who are likely to shoplift, can also contribute to the racial profiling of Black people that already occurs without any algorithmic help.[154] Other commercial uses may pose repeated inconvenience, embarrassment, hassle, or other significant problems that cannot be accepted as an inevitable side effect.

Being unable to access one's smartphone, bank account, or apartment is not a trivial inconvenience that people can brush aside as unfortunate wrinkles insufficient to outweigh the overall value of a service that provides additional convenience for others. The ways in which facial recognition technologies enable discrimination by poor accuracy for faces of certain demographic groups threaten the privacy, well-being, prosperity, and safety of those people simply by virtue of who they are.

[151] *See* Keyes, *supra* note 127, at 88:6-8 (surveying the available literature and finding the analysis and research relating to the response of facial recognition systems to trans people as severely wanting, "Papers near-uniformly fell into one of these two types of statement; either they would explicitly come out and claim that gender was a binary classification problem, or contained two categories, or they would commonly describe their dataset labels as only containing male/female or man/woman options, without any mention that this might be missing something.").

[152] *See* MIRANDA BOGEN & AARON RIEKE, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS 36 (Dec. 2018); Buolamwini & Gebru, *supra* note 125.

[153] *See* Buolamwini & Gebru, *supra* note 125.

[154] Cassi Pittman, *"Shopping While Black": Black Consumers' Management of Racial Stigma and Racial Profiling in Retail Settings*, 20(I) J. CONSUMER CULTURE 3, 9 (2017), https://journals.sagepub.com/doi/pdf/10.1177/1469540517717777; Michelle Singletary, *Shopping While Black. African Americans Continue to Face Retail Racism.*, WASH. POST (May 17, 2018, 7:46 AM), https://www.washingtonpost.com/news/get-there/wp/2018/05/17/shopping-while-black-african-americans-continue-to-face-retail-racism/ [https://perma.cc/6E8X-9CV7].

Child-Specific Harms

Young people are another group for whom facial recognition technologies are more likely to be inaccurate, and for whom the use of those technologies poses risks distinct to them on the basis of their physical characteristics.[155] Children often have even less control over their privacy than adults do, and facial recognition surveillance frequently targets children out of misguided attempts to protect them.[156] The chill to free expression that results from awareness of surveillance through facial recognition may also have a particularly significant impact on their emotional and intellectual development. The fact that facial recognition technologies perform less accurately for children's faces puts them at risk when law enforcement or school security systems use the technology. Many of these harms are similarly applicable to and deeply concerning for adults, but may be even more severe for children due to their immaturity and the fact that childhood and adolescence are tremendously formative for both identity and opportunities later in life.

In some cases, facial recognition may be even more unavoidable for young people than it is for adults. Children, and to some extent adolescents, often do not have control over their movements or how parents or schools disseminate pictures of them. There is of course some basis for that—autonomy is tied to the maturity required to safely exercise it, and the law provides parents with decision-making rights over their young children in all kinds of ways.[157] But children are being subjected to facial recognition technology in schools, at summer camp, at daycare, and in places where adults are also surveilled (like church, their apartment building, or in public).[158] Concerns about safety in schools have helped facial recognition grow in popularity in schools, which children are, with a few exceptions, legally required to attend.[159] Children also have their pictures taken by adults, some of whom upload them to social media without understanding the full ramifications.[160] My objective is not to blame every parent who has ever uploaded a picture of their child—sharing pictures of one's children is a natural instinct. But when children's pictures are widely disseminated online,

[155] *See* SONIA LIVINGSTONE ET AL., CHILDREN'S DATA AND PRIVACY ONLINE: GROWING UP IN A DIGITAL AGE 25 (London School of Economics and Political Science 2019).

[156] *See* Gary T. Marx & Valerie Steeves, *From the Beginning: Children as Subjects and Agents of Surveillance*, 7(3/4) SURVEILLANCE & SOC'Y 192, 192 (2010) ("Kids are literally the poster children for surveillance.").

[157] LIVINGSTONE ET AL., *supra* note 155, at 12-13.

[158] Claire Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, CTR. ON PRIVACY & TECH. (May 15, 2019), https://www.americaunderwatch.com/ [https://perma.cc/KNQ9-TS75].

[159] *See* Leslie Regan Shade & Rianka Singh, *"Honestly, We're Not Spying on Kids": School Surveillance of Young People's Social Media*, SOCIAL MEDIA + SOC'Y 1, 1-2 (discussing how safety considerations have driven the trend of surveilling children in schools).

[160] LIVINGSTONE ET AL., *supra* note 155.

anyone who obtains access to them may use the photos, including for the purpose of adding pictures of children to facial recognition databases.

Ironically, children may be at particular risk of having their pictures added to facial recognition databases without their knowledge or permission out of attempts to improve facial recognition algorithms' ability to accurately recognize them.[161] As companies and governments try to improve their datasets and algorithms, they will focus on obtaining pictures from populations poorly represented in them, such as children or adults with darker skin.[162] In one particularly horrifying example, the National Institute of Standards and Technology resorted to using images of children who were exploited for child pornography in order to build a sufficiently robust database of children's faces as part of an evaluation of popular facial recognition algorithms.[163]

Moreover, concern over children's safety, and the broad consensus that measures intended to keep them safe are desirable, may lead to particular focus on children when it comes to uses of facial recognition technologies designed to either keep track of children or find ones in danger.[164] Amazon's announcement that it would prohibit law enforcement use of its facial recognition service Rekognition for one year provides an example of how the dangers of facial recognition can be distinguished when it comes to deployment on children for

[161] Kashmir Hill & Aaron Krolik, *How Photos of Your Kids Are Powering Surveillance Technology*, THE N.Y. TIMES (Oct. 11, 2019), https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html [https://perma.cc/WT2F-2H9U] ("Importantly to the University of Washington researchers, MegaFace included children like Chloe and Jasper Papa. Face-recognition systems tend to perform poorly on young people, but Flickr offered a chance to improve that with a bonanza of children's faces, for the simple reason that people love posting photos of their kids online.").

[162] Drew Harwell, *AI Baby Monitors Attract Anxious Parents: 'Fear is the Quickest Way to Get People's Attention,'* WASH. POST (Feb. 25, 2020, 7:00 AM), https://www.washingtonpost.com/technology/2020/02/25/ai-baby-monitors/ [https://perma.cc/NZ6X-HJJF]; Sean Hollister, *Google Contractors Reportedly Targeted Homeless People for Pixel 4 Facial Recognition*, THE VERGE (Oct. 2, 2019, 8:46 PM), https://www.theverge.com/2019/10/2/20896181/google-contractor-reportedly-targeted-homeless-people-for-pixel-4-facial-recognition [https://perma.cc/72YC-2W4R].

[163] Os Keyes et al., *The Government is Using the Most Vulnerable People to Test Facial Recognition Software*, SLATE (Mar. 17, 2019, 8:32 PM), https://slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html [https://perma.cc/CGQ3-LREM].

[164] *See, e.g.*, Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020, 3:43 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/2K95-RYZY] (finding Clearview AI uses facial recognition technology in human trafficking investigations).

their purported protection.[165] The company specifically exempted use by organizations to "to help rescue human trafficking victims and reunite missing children with their families."[166] Similarly, Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children,[167] including investigations into child sexual exploitation.[168] The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified. Yet the gravity of those crimes, and the desire of all relevant stakeholders to prevent, discover, halt, and deter their occurrence, may lead to facial recognition technologies being deployed in that context with some frequency or that context being exempted from certain reforms.

Developmental Limitations

When it comes to privacy, advertising, and the ability to contract, there is a strong tradition in the law of recognizing children's immaturity and vulnerability due to their age.[169] As privacy-invasive technologies have adopted a larger and more impactful role in children's lives, research from a range of disciplines including sociology, media studies, and engineering has examined children and adolescents' privacy attitudes and coping strategies.[170] Given the relative newness of facial recognition technologies (and most likely, the necessary logistical

[165] *We Are Implementing a One-Year Moratorium on Police Use of Rekognition*, AMAZON (June 10, 2020), https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [https://perma.cc/P9Z4-KQGU].

[166] *Id.*

[167] Steven Musil, *Clearview AI still backs facial recognition, despite competitors' concerns*, CNET (June 10, 2020, 6:10 PM), https://www.cnet.com/news/clearview-ai-still-backs-facial-recognition-despite-competitors-concerns/ [https://perma.cc/9AY8-Y4XG] ("Clearview CEO Hoan Ton-That says his company's technology can help protect children and victims of crimes, without risk of racial bias, singling out competitor Amazon's Rekognition as failing in that regard."); Hill & Dance, *supra* note_3 ("In numerous publicity documents, Clearview promotes the use of its technology by law enforcement to solve child sexual abuse cases.").

[168] Hill & Dance, *supra* note 3.

[169] LIVINGSTONE ET AL., *supra* note 155, at 4, 28, 34-35.

[170] *See, e.g.,* Andrew Hope, *Seductions of Risk, Social Control, and Resistance to School Surveillance*, *in* SCHOOLS UNDER SURVEILLANCE: CULTURES OF CONTROL IN PUBLIC EDUCATION 230 at 233, 235, 237, (Torin Monahan & Rodolfo D. Torres eds., Rutgers Univ. Press 2010) (discussing different methods of student monitoring and students' perceptions and reactions to it); LIVINGSTONE ET AL., *supra* note 155, at 8-9, 15 *("*While the commercial use of children's data is at the forefront of current privacy debates, the empirical evidence lags behind, with very few studies examining children's awareness of commercial data gath-

difficulties involved with doing ethical research on children), only a few studies focus on the impact of facial recognition specifically, and more research is sorely needed. Until then, research on young people's attitudes about online privacy risks are instructive given how companies scrape pictures from the internet to fuel facial recognition databases, while research about their reactions to real-time video surveillance can inform how they may react to those uses of facial recognition and analysis.[171]

In terms of broader privacy attitudes and perceptions, studies have found that children have a range of perspectives and capacities to comprehend privacy risks, but tend to focus more on interpersonal privacy violations, such as if a parent can view something they've posted, rather than on privacy invasions by corporations or the government.[172] For example, a 13-year-old in one study explained that she considered Facebook to be public and Twitter private, because she knew that her peers maintained Facebook accounts and would see what she posted, when that was less likely to be true of Twitter.[173] Young people have privacy concerns, but may not be as concerned about corporate exploitation, including the collection and use of any photos they post by companies, and are less able to accurately gauge comparative risks. Young children also struggle with correctly assessing different types of privacy risks, such as the importance of not disclosing sensitive information publicly as opposed to correctly evaluating privacy risks.[174] A poor understanding of the nuances of various privacy risks makes children vulnerable to their privacy being exploited online, including by having the pictures they post collected and used in facial recognition databases. The relative popularity with young people of social media platforms that focus on user-posted photos and videos, like TikTok, Instagram, and Snapchat, also gives the companies operating those applications and any third parties they share data with frequent opportunities to collect images of children's faces.[175]

ering and its implications."); Michael McCahill & Rachel Finn, *The Social Impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums,'* 7 (3/4) SURVEILLANCE & SOC'Y, 273, 278 (2010) (evaluating students' perception of surveillance, including through the use of CCTV and biometrics such as a thumbprint, but not facial recognition).

[171] Andrejevic & Selwyn, *supra* note 15, at 115-17 (reviewing the growth of facial recognition technology in schools and relevant literature).

[172] LIVINGSTONE ET AL., *supra* note 155, at 12, 23, 25 ("Online spaces, while technically public, can be experienced as offering greater 'privacy' because they are parent-free compared with, for example, what a child can say or do at home.").

[173] *Id.* at 12; *see also* Marx & Steeves, *supra* note 156, at 213.

[174] Jun Zhao et al., *'I Make Up A Silly Name': Understanding Children's Perception of Privacy Risks Online* in CHI '19: PROC. OF THE 2019 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS. 1, 2 (2019).

[175] *See* Rebecca Jennings, *The Not-So-Secret Life of a TikTok-Famous Teen*, VOX (Oct. 2, 2019, 8:30 AM), https://www.vox.com/the-goods/2019/10/2/20891915/tiktok-famous-teenagers-haley-sharpe-yodeling-karen [https://perma.cc/U54D-DR45]; Taylor Lorenz, *Teens Are Being Bullied 'Constantly' on Instagram*, THE ATLANTIC (Oct. 10, 2018),

This disproportionate focus on interpersonal privacy and lack of understanding of corporate (or governmental) surveillance also extends to teenagers.[176] A lack of awareness of how their data is being collected combined with a desire to connect with their peers on social media can also make young people vulnerable to having their photos collected for a facial recognition database simply because they wanted to communicate with their friends. In fact, one study of teenagers' privacy perceptions and concerns found that while the teens tended to report a general concern about being identified by data collected from them, they failed to accurately gauge the risks of disclosing information themselves, including photographs.[177]

Children and teens being unaware that using Facebook to bond with their friends puts them at risk of their pictures being shared with law enforcement[178] is precisely why we have consumer protection, criminal, and other doctrines in various areas of law that create allowances for immaturity. There are compelling reasons why this kind of commercial surveillance cannot be fairly attributed to informed assumption of the risk for adults in many circumstances. But it is particularly unconscionable for companies to take advantage of young people whose decision-making capabilities make them even more even more poorly equipped to protect themselves from commercial and governmental intrusion.

Conversely, awareness of surveillance also has repercussions for young people distinct from ignorance or confusion. When teenagers are aware and concerned about online surveillance, some choose not to participate in online activity, such as by refraining from using social media altogether or otherwise modifying their online behavior.[179] While abstention would shield them from privacy invasions, it also prevents them from bonding with their peers online, which is an increasingly substantial component of many adolescent social interactions.[180] A study by Alice Marwick and danah boyd of teenagers from low-

https://www.theatlantic.com/technology/archive/2018/10/teens-face-relentless-bullying-instagram/572164/ [https://perma.cc/6JMW-Y46C]; Taylor Lorenz, *Posting Instagram Sponsored Content is the New Summer Job,* THE ATLANTIC (Aug. 22, 2018), https://www.theatlantic.com/technology/archive/2018/08/posting-instagram-sponsored-content-is-the-new-summer-job/568108/[https://perma.cc/7CU2-Q79X]; Monica Anderson & Jingjing Jiang, *Teens' Social Media Habits and Experiences*, PEW RES. CTR. (Nov. 28, 2018), https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/ [https://perma.cc/8ACP-HZ4P].

[176] Marwick & Boyd, *supra* note 4, at 1056.

[177] Zhao et al., *supra* note 174, at 2.

[178] Hill, *supra* note 51.

[179] Alice Marwick et al., *"Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth*, SOC. MEDIA + SOC'Y 1, 5 (2017).

[180] Joanna C. Yau & Stephanie M. Reich, *"It's Just a Lot of Work": Adolescents' Self-Presentation Norms and Practices on Facebook and Instagram*, 29 J. OF RES. ON ADOLESCENCE 196, 196 (noting the prominence of social media in adolescent social norms and the importance of social media for "identity exploration and construction").

income backgrounds found a range of privacy awareness, savviness, and concerns, including a general awareness that whatever information they post online can have reputational or professional ramifications for them later in life. They also observed a heavy undercurrent of victim-blaming for privacy violations.[181]

Similarly, researchers who examined how adolescents' approach to self-presentation on social media impacts their identity formation documented scrupulous self-awareness in spaces where adolescents knew it was likely their peers could see what they posted, as opposed to anonymous formats like blogs where they can explore new subjects and identities without fear of criticism or rejection by peers.[182] Young people use social media to bond with their peers and discover more about the world at crucial development stages, and justified fears of surveillance could limit their ability to make those relationships and seek out important information, or at the very least mold how they approach those things in ways we do not currently understand.[183]

Research on CCTV surveillance can be instructive for the impact real-time facial recognition surveillance may have on young people, including disparate effects based on gender and class. A UK study on students' reactions to CCTV surveillance found that knowledge of the cameras produced a range of responses from students: for some it has a chilling effect, as they were concerned the cameras might misinterpret their actions, while others attempted to avoid the surveillance or obfuscate their conduct so that it would be misinterpreted.[184] Gender and class also appeared to impact the children's responses: children from wealthier neighborhoods noted that they had did not mind public CCTV cameras because "they weren't doing anything wrong,"[185] while girls frequently reported concerns about voyeurism and that constant surveillance facilitated a need to look "perfect."[186]

Real-time monitoring of the spaces children inhabit will likely impact how they behave and how they think of themselves, and knowledge of their privacy being invaded online may have similar effects. As Livingstone et al note in their comprehensive literature review of existing research on children's privacy perceptions and literacy, much work is left to be done on how children's development is impacted by a lack of privacy, and the distinctions between how children respond at different ages.[187] McCahill and Finn also note that further work is

[181] Marwick et al., *supra* note 179, at 9-11.

[182] Yau & Reich, *supra* note 180, at 206.

[183] *Id.* at 196-7, 206.

[184] McCahill & Finn, *supra* note 161, at 273, 283-84.

[185] *Id.* at 279.

[186] *Id.* at 287.

[187] *See* LIVINGSTONE ET AL., *supra* note 155.

needed on the impact of surveillance on children's identity formation in particular.[188] But the research that exists suggests that children's understanding and reactions to surveillance warrants careful scrutiny of introducing surveillance into their lives for their purported benefit.

Bias and Inaccuracies

Researchers have also found that facial recognition algorithms perform less accurately on the faces of young people. The National Institute of Standards and Technology, which runs a series of periodical evaluations of facial recognition algorithms, found higher rates of false positives for children and the elderly in its most recent study, with the highest rates among those for the youngest children and the oldest adults.[189] People aged 12-20 produced high false match rates, and the dataset did not include individuals below the age of 12.[190] The report concluded that aging, as it changes one's appearance over the course of decades, "will ultimately undermine automated face recognition."[191] It's intuitive that an algorithm trained to verify the identity of a 12-year-old would might return a false negative on images of the child at, for example, 15, when the shape of their face that the program learned to recognize has changed.

The NIST results echo what little other work there is on the accuracy of facial recognition algorithms on young faces. A 2019 study tested eight facial recognition systems and found that they performed more poorly for children than adults on both one-to-one and one-to-many searches.[192] An earlier study found that age variation—the age of the subject in the probe image compared to the age of the subject in the database image—heavily impacted the accuracy of facial recognition algorithms used on children, particularly younger children.[193] While much more work is needed, evaluations of how facial recognition algorithms assess children have generally shown that the existing systems are often inaccurate for young faces.

[188] McCahill & Finn, *supra* note 170, at 286, 288 ("These findings suggest that it may be useful for future research, including our own, to situate the 'subjective experiences' and 'behavioural responses' of the 'surveilled' in a wider context by drawing upon sociological theories on 'identity formation' in 'late modernity'. . .By evading, negotiating and resisting surveillance regimes, the children also shaped surveillance practices and technologies in novel and unanticipated ways.").

[189] GROTHER ET AL., *supra* note 28, at 8.

[190] *Id.* at 51.

[191] *Id.* at 17.

[192] NISHA SRINIVAS ET AL., FACE RECOGNITION ALGORITHM BIAS: PERFORMANCE DIFFERENCES ON IMAGES OF CHILDREN AND ADULTS 5-6 (Comput. Vision Found. 2019).

[193] DANA JACLYN MICHALSKI, THE IMPACT OF AGE-RELATED VARIABLES ON FACIAL COMPARISONS WITH IMAGES OF CHILDREN: ALGORITHM AND PRACTITIONER PERFORMANCE 161 (Univ. of Adelaide 2017).

Inaccurate facial recognition systems that make it more likely for young people to become erroneously involved in a law enforcement investigation pose severe risks to young people, particularly young people of color, given how contact with the criminal justice system can threaten their current and future well-being, health, educational and professional prospects, and freedom. In 2019, the Georgetown Center on Privacy & Technology obtained records demonstrating that the NYPD had been using thousands of juvenile mug shots in a facial recognition database in order to compare them to crime scene images, including children as young as 11.[194] The decision to use the system on mug shot images of children and teens was approved by the NYPD's legal department, but was not disclosed to oversight authorities like the City Council, nor to the public.[195] As of August 2019, there were photos of 5,500 individuals in the database, and the NYPD would not provide statistics on how often their system provided false matches.[196] Furthermore, it is unclear how many other police departments are doing the same thing, as few have public-facing facial recognition policies.[197] Putting children into facial recognition systems that are likely to misidentify them puts them at risk of being wrongly accused of a crime. At the same time, systemic problems like the failure of procedural protections for young people and the need for children to make crucial legal decisions without an attorney can make it harder for them to defend themselves and emerge from the encounter unscathed.[198]

These risks are far more dire for children of color. Black youth are a cataclysmic *500%* more likely to be detained or committed than their white peers,[199] and they are more likely to be sent to adult prisons and receive longer sentences than their peers, even when accounting for the type of offense.[200] This puts them further at risk, as youth who are tried as adults and sent to adult prisons are more likely to commit suicide in jail, exhibit psychiatric symptoms, and re-offend upon release.[201] While there is scant, if any, research on how facial recognition algorithms assess children of color specifically, the inability of these systems to assess adults with darker skin and children makes it more likely that there would be additional errors in evaluating children of color.

[194] Goldstein & Watkins, *supra* note 8.

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *See* AM. CIVIL LIBERTIES UNION ET AL., A CALL TO AMEND THE OHIO RULES OF JUVENILE PROCEDURE TO PROTECT THE RIGHT TO COUNSEL 2-3 (2006).

[199] THE SENTENCING PROJECT, FACT SHEET: LATINO DISPARITIES IN YOUTH INCARCERATION (2017).

[200] JEREE MICHELE THOMAS & MEL WILSON, THE COLOR OF YOUTH TRANSFERRED TO THE ADULT CRIMINAL JUSTICE SYSTEM: POLICY AND PRACTICE RECOMMENDATIONS 1 (Nat'l Ass'n of Soc. Workers 2017).

[201] *Id.* at 4.

These mutually reinforcing risk factors for children of color in particular also illustrate why the use of facial recognition systems in schools is so corrosive. While the understanding that their movements are being surveilled in real time will likely have chilling effects on the intellectual and emotional development of all children, inaccurate assessments of children of color could help exacerbate the school-to-prison pipeline, or the effects of a punitive approach to school discipline that results in higher arrest and incarceration rates for the children subject to it, particularly poor children and children of color.[202]

EXISTING LAWS ARE INSUFFICIENT

Were any of the existing legal protections designed to guard against the harms identified adequate to mitigate them, a full ban on the use of facial recognition technologies might not be necessary. But even as certain applicable laws present narrow potential remedies, none of them are sufficient to tackle the dangers that facial recognition technologies present for individual groups and for society as a whole. Inapt definitions, underenforcement by regulators of laws that lack private rights of action, and the difficulty of making private rights of action meaningful avenues for vindicating privacy violations are common threads throughout relevant privacy laws, civil rights laws, and children's privacy laws.[203] None of these protections have been sufficient to guard against the dangers of facial recognition so far, and even where specific laws could help correct a narrow part of the problem, there is no reasonable case to be made that the existing laws in our system *will* be capable of tackling every part of the problem.

Quasi-Universal Harms: Comprehensive & Sectoral Privacy Protections

American privacy laws have been broadly decried as overly permissive, overly procedural, and ill-equipped to grapple with the realities of modern technology,[204] critiques that are robustly applicable to the use of facial recognition technologies by both companies and the government. The United States lacks a comprehensive, federal consumer privacy law, and the sector-specific federal consumer privacy laws it has often fail to reach the most problematic practices,

[202] *See* Amy G. Halberstadt et al., *Preservice Teachers' Racialized Emotion Recognition, Anger Bias, and Hostility Attributions*, 54 CONTEMP. EDUC. PSYCHOL. 125, 128 (2018) (discussing research reporting that teachers are more likely to perceive faces of Black children as angry than faces of white children).

[203] *See, e.g.*, Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 575-78 (2017).

[204] *See, e.g.*, Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 356 (2015); Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 6 (2019); William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 973-75 (2016).

or are under-enforced by regulators.[205] A robust lobbying industry funded by enormously wealthy tech companies makes it difficult for tougher privacy laws to be enacted at the state or federal levels,[206] and the combination of few applicable laws and laws that aren't robustly enforced when they do apply has created terrible incentives for companies to violate people's privacy.

The United States also lacks a consumer agency focused exclusively on technology and privacy, relying instead on the Federal Trade Commission (FTC), state Attorneys General,[207] and a few other federal agencies to regulate and enforce consumer privacy laws.[208] Both the FTC and the state Attorneys General have unfairness and deceptive practices authorities that they use to curb dangerous privacy and data security practices when a more sector-specific authority does not apply.[209]

While at least partially attributable to a lack of sufficient legal authorities and resources, the FTC has done an uneven job at protecting Americans' privacy,[210] including its oversight of facial recognition technologies. As an example, the FTC found that Facebook made it impossible for some users to opt out of facial recognition technology being used on the photographs they posted on the platform, and the agency included that finding in its 2019 settlement with Facebook for its alleged violations of a 2012 consent order.[211] The failure to allow some users to opt out of having facial recognition used on them was one of a long series of allegations concerning the company's providing data from millions of people to Cambridge Analytica, resulting in Facebook agreeing to monitoring

[205] *See generally* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1065-1081 (2019) (outlining the critiques of American consumer privacy law).

[206] *See* Alvaro M. Bedoya, *Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html [https://perma.cc/MB2L-YPLM]; *see also* Barrett, *supra* note 205, at 1067, n.47 (describing tech companies' strategy of "cooperation . . . to stave off more significant regulatory intervention" by the government).

[207] *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 749-50 (2016).

[208] *See, e.g.*, Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the* CFPB, 2 GEO L. TECH. REV. 531, 544; *Customer Privacy*, FCC (last visited June 20, 2020), https://www.fcc.gov/general/customer-privacy [https://perma.cc/8PF5-ZCKC].

[209] McGeveran, *supra* note 204, at 977.

[210] Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is The FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 516, 530 (2018).

[211] *See* Facebook, Inc., F.T.C. No. C-4365 (2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf [https://perma.cc/EUE9-LRQ8]; Thomas Germain, *Facebook Updates Facial Recognition Settings After CR Investigation*, CONSUMER REPORTS (Sept. 3, 2019), https://www.consumerreports.org/privacy/facebook-updates-facial-recognition-setting/ [https://perma.cc/7XPM-82HG].

requirements and a five-billion-dollar fine.[212] The lack of meaningful injunctive relief and the paucity of the fine relative to Facebook's coffers led to widespread criticism of the settlement, and of the specific and general incentives it created.[213] One can find few clearer indictments of the perverse incentives that weak enforcement has created than the fact that the day the settlement was first reported, Facebook's stock went up.[214] The FTC has provided guidance on best practices for the use of facial recognition technologies,[215] but has not brought any enforcement cases involving facial recognition other than the Facebook settlement, despite a number of detailed requests for the agency to investigate various companies brought by various consumer groups over the years.[216] The guidance also does not address potential biases, due process problems, or free expression concerns.

[212] *See* Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/GB8S-KM3F].

[213] *See, e.g.*, Devin Colway, *9 reasons the FTC settlement is a joke*, Tech Crunch (July 24, 2019, 8:01 PM), https://techcrunch.com/2019/07/24/9-reasons-the-facebook-ftc-settlement-is-a-joke/ [https://perma.cc/D9SX-5BKM]; Editorial Board, *A $5 Billion Fine for Facebook Won't Fix Privacy*, N.Y. TIMES (July 25, 2019), https://www.nytimes.com/2019/07/25/opinion/facebook-fine-5-billion.html; Rep. Frank Pallone, *Pallone Statement on the FTC's Facebook Settlement*, HOUSE COMMITTEE ON ENERGY & COMMERCE (July 24, 2019), https://energycommerce.house.gov/newsroom/press-releases/pallone-statement-on-the-ftc-s-facebook-settlement [https://perma.cc/5WL6-JAE7] ("While $5 billion is a record fine for the FTC, monetary damages are not enough."); Nilay Patel, *Facebook's $5 billion FTC fine is an embarrassing joke*, The Verge (July 12, 2019, 9:05 PM), https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke [https://perma.cc/6SRM-2S3H]; Adam Schwartz, *The FTC-Facebook Settlement Does Too Little To Protect Your Privacy*, EFF (July 24, 2019), https://www.eff.org/deeplinks/2019/07/ftc-facebook-settlement-does-too-little-protect-your-privacy [https://perma.cc/RUS5-UQKU]; Siva Vaidhyanathan, *Billion-dollar fines can't stop Google and Facebook. That's peanuts for them,* The Guardian (July 26, 2019, 6:00 AM), https://www.theguardian.com/commentisfree/2019/jul/26/google-facebook-regulation-ftc-settlement [https://perma.cc/7TTQ-4G38].

[214] Carla Herreria Russo, *Critics Say Facebook Penalty Is A Slap On The Wrist As Stock Prices Surge*, HUFFPOST (July 7, 2012, 11:37 PM), https://www.huffpost.com/entry/critics-ftc-facebook-fine_n_5d2923fce4b0bd7d1e1c763c?guce [https://perma.cc/H53G-KYNW].

[215] *See generally* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USE OF FACIAL RECOGNITION TECHNOLOGIES (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/U78A-8A64].

[216] *See In re Facebook and Facial Recognition (2018)*, EPIC, https://epic.org/privacy/ftc/facebook/facial-recognition2018/ [https://perma.cc/7TKN-CGUH]; *see also* Complaint and Request for Investigation, Injunction, and Other Relief Submitted by The Electronic Privacy Information Center (EPIC) at 1, In the Matter of HireVue, Inc. (2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf

The FTC has also tended to focus its privacy enforcement on its deception authority, which can be a somewhat weak tool against abusive practices. Prohibiting deceptive practices makes lying about data practices illegal, but not the practices themselves.[217] In contrast, the FTC's unfairness authority forbids companies from engaging in practices that cause "substantial" injury to consumers that the consumer could not easily avoid and that is not "outweighed by any countervailing benefits to consumers or competition."[218] The authority that makes a normative claim about the value and harms of the practice, not simply whether the company has lied about its deployment, would seem to be a better fit to meaningfully curb the use of facial recognition technologies, though the FTC tends to rely more heavily on its deception authority and thus might be less likely to act on such a theory.[219]

The effects of inadequate consumer privacy laws on how facial recognition technologies are used are not limited to the consumer sphere: a lack of consumer guardrails also make more data available for law enforcement perusal, and normalizes invasive uses of these technologies by the police.[220] Even more concretely, companies that supply law enforcement with technology are subject to the perverse incentives of an underregulated marketplace just as other companies are.[221] Clearview AI was privately urging law enforcement customers to use their product on family and friends, while publicly stating that its service was confined to on-the-job enforcement uses in its code of conduct.[222]

[https://perma.cc/2SCM-KJVF]; John D. McKinnon, *Facebook's Facial Recognition Feature Violates Users' Privacy Rights, Groups Allege*, WALL ST. J. (Apr. 6, 2018, 10:32 AM), https://www.wsj.com/articles/consumer-groups-file-ftc-complaint-against-facebook-1523025141 [https://perma.cc/4QVU-6GAA].

[217] *See* G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 165, 171-72 (2012).

[218] FED. TRADE COMM'N, FTC POLICY STATEMENT ON UNFAIRNESS (1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/FJV4-GEKM].

[219] *See* Nicholas Confessore & Cecilia Kang, *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites*, N.Y. TIMES (Dec. 30, 2018), https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html [https://perma.cc/XD3L-MSX2].

[220] *See, e.g.*, Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html [https://perma.cc/BKY8-ACCF] ("Ubiquitous mass surveillance is increasingly the norm. . . . In countries like the United States, it's being built by corporations in order to influence our buying behavior, and is incidentally used by the government.").

[221] *See, e.g.*, Mac et al., *supra* note 164 (explaining that Clearview acknowledged that a public version of their product, in contrast to the current version available only to law enforcement agencies, would be more profitable).

[222] *Id.*

Ultimately, the consumer protection laws that govern companies collecting Americans' photographs and running facial recognition systems enable law enforcement violations of people's privacy because law enforcement agencies frequently rely on consumer-facing products and platforms.[223] A company like Clearview AI exists because social media and other companies that collect people's photographs have few, if any, deletion or retention requirements, while inadequate regulations and enforcement thereof incentivize companies to exploit their customers and violate their privacy.[224] Companies collect and hoard whatever data they can find with minimal risk of regulatory repercussions, and the databases and products they build are then available for law enforcement perusal.[225] Facial recognition technologies, perhaps better than any other, illustrates how corporate and government data collection and use practices are often deeply intertwined, with the failure of consumer regulation fueling what law enforcement is able to access.[226]

A few state consumer privacy laws apply to facial recognition but are limited in scope, efficacy, and definitionally, jurisdiction. Three states have biometric-specific privacy laws: Illinois, Texas, and Washington, though the Washington state law does not include facial geometry in its definition of biometric identifiers, and it explicitly excludes "a physical or digital photograph, video or audio recording or data generated therefrom."[227] It is thus unclear, and has yet to be determined by a court, whether the Washington state law applies to the use of facial recognition.[228] Like the Texas and Illinois statutes, the Washington law predicates its protections on consent, which is a broken paradigm particularly ill-suited for regulating technologies that people are typically unaware are being used on them at all.[229]

[223] *See* Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html [https://perma.cc/YA39-A9ZS].

[224] *See* Barrett, *supra* note 205, at 1077-78.

[225] Lindsey Barrett, *Carpenter's Consumers*, 59 WASHBURN L.J. 53, 54 (2002).

[226] *See id.* at 54, 72.

[227] WASH. REV. CODE § 19.375.010 (2020). Data breach laws in other states, like Arkansas, Wisconsin, Iowa, Wyoming, and Nebraska, define "personal information" to include biometrics like facial geometry. ARK. CODE ANN. § 4-110-103 (2019) (LexisNexis); IOWA CODE § 715C.1 (2020); NEB. REV. STAT. § 87-802 (2020); WIS. STAT. § 134.98 (2020); WYO. STAT. ANN. § 40-12-501 (2020). *See generally* Thomas F. Zych et al., *State Biometric Privacy Legislation: What You Need to Know*, LEXOLOGY (Sept. 5, 2019), https://www.lexology.com/library/detail.aspx?g=ebc0e01c-45cc-4d50-959e-75434b93b250 [https://perma.cc/2L6K-CPSB] (outlining states' regulations on biometric data).

[228] *Washington Becomes Third State to Enact Biometric Privacy Law*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SEC. LAW BLOG (June 1, 2017), https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/ [https://perma.cc/A4WR-D2LT].

[229] 740 ILL. COMP. STAT. 14/15 (2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019); WASH. REV. CODE § 19.375.020 (2020).

The Texas and Illinois statutes require private entities to provide notice and obtain consent from the data subject before collecting a biometric identifier from them, though the Texas statute is more permissive in a number of ways.[230] In the Texas law, the requirement for obtaining notice and consent is limited to collection for a "commercial" purpose, consent need not be written, and unlike under the Illinois law, sale and lease of the data is permitted with consent.[231] Crucially, the Texas statute is only enforceable by the state Attorney General, while the Illinois statute includes a private right of action for individuals to vindicate violations.[232] The lack of private right of action, in addition to its narrower definitions, makes the Texas law a much less meaningful source of privacy protections, and has been fairly described as more "industry-friendly."[233]

These state laws, particularly the one in Illinois, are a step in the right direction, but none of them are sufficient to compensate for the remaining gaps in federal law and enforcement.[234] Consent is a minimal procedural protection, and the requirement to obtain it is unlikely to limit the use and spread of facial recognition technologies absent other factors.[235] The Illinois law's private right of action and steep fines have forced companies to be more thoughtful about how they collect and use biometric identifiers in that state and have resulted in litigation significant enough for companies to take it seriously,[236] but the law could benefit from more granular limitations on uses of biometrics once consent has

[230] 740 ILL. COMP. STAT. 14/15 (West 2019); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

[231] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

[232] 740 ILL. COMP. STAT. 14/20 (West 2019); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

[233] Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C. J.L. & TECH. 161, 176-77 (2018).

[234] *See* Mason Kortz, *Facial Recognition Regulation – A Year in Review*, AM. CONST. SOC'Y: EXPERT FORUM (Dec. 17, 2019), https://www.acslaw.org/expertforum/facial-recognition-regulation-a-year-in-review/ [https://perma.cc/SCP7-ZQ3Z] ("Progress at the state and local level doesn't obviate the need for federal legislation though.").

[235] *See* Crystal Lee and Jonathan Zong, *Consent is Not an Ethical Rubber Stamp*, SLATE (Aug. 30, 2019, 7:30 AM), https://slate.com/technology/2019/08/consent-facial-recognition-data-privacy-technology.html [https://perma.cc/GLU6-V9GL] ("[C]licking the "accept" button often gives companies carte blanche to use your private data, and it's frequently impossible to know where your data will go. Like the tobacco companies that preceded them, companies like Amazon and Facebook can argue that you've made an informed choice: You consented to their terms of service and willingly uploaded the photos, so you can't blame them for the results.").

[236] Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [https://perma.cc/LFY2-5FXN].

been obtained. None of these state laws constrain government or law enforcement collection or use of biometric identifiers,[237] and these state laws are, by their definition, jurisdiction-limited. Jurisdiction-limited laws can have an outsized effect when the size of the jurisdiction's market makes multiple standards impracticable for companies, as exemplified by the impact of California's passage of California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR).[238] Illinois, however, does not appear to have had that effect.[239] None of these biometric-centric laws obviate the need for a comprehensive ban.[240]

Unfortunately, the laws that specifically apply to law enforcement use of facial recognition also fail to curb its use or mitigate the harms it inflicts. Scholars including Catherine Crump and Elizabeth Joh have written about how opaque police procurement policies enable the acquisition and deployment of facial recognition systems that have not been vetted or approved by oversight organizations or the public.[241] Police departments in the San Diego area, for example, started developing and deploying a facial recognition system in 2007 without disclosing it to the public until 2013.[242] The departments stopped using the program—tablets and devices that officers carried in the field, which would compare photographs the officer took to a centralized database[243]—last year, with a spokesperson for the department reporting that they were unaware of the technology leading to a single successful arrest or prosecution.[244]

Constitutional protections have also served as an inadequate check on law enforcement deployments of facial recognition technologies. The Fourth

[237] *See, e.g.*, TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019) (explicitly permitting companies to provide biometric data to a law enforcement agency possessing a warrant).

[238] Caitlin Chin, *Highlights: The GDPR and CCPA as Benchmarks for Federal Privacy Legislation*, BROOKINGS: TECHTANK (Dec. 19, 2019), https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/ [https://perma.cc/ND3M-Q7J2].

[239] Lori Tripoli, *Resurgent BIPA more than a second fiddle to CCPA?*, COMPLIANCE WEEK (Feb. 21, 2020, 11:36 AM), https://www.complianceweek.com/data-privacy/resurgent-bipa-more-than-second-fiddle-to-ccpa/28481.article [https://perma.cc/QP4S-P556].

[240] *See* discussion *infra* Section V(i).

[241] Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH L. REV. 1595 (2016); Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 101 (2017).

[242] Crump, *supra* note 241, at 1629.

[243] Dave Maass, *Victory: San Diego to Suspend Face Recognition Program, Limits ICE Access to Criminal Justice Data*, ELECTRONIC FRONTIER FOUND. (Dec. 11, 2019), https://www.eff.org/deeplinks/2019/12/victory-san-diego-suspend-face-recognition-program-cuts-some-ice-access [https://perma.cc/B9TT-X8U9].

[244] DJ Pangburn, *San Diego's Massive, 7-Year Experiment eith Facial Recognition Technology Appears to be a Flop*, FAST COMPANY (Jan. 9, 2020), https://www.fastcompany.com/90440198/san-diegos-massive-7-year-experiment-with-facial-recognition-technology-appears-to-be-a-flop [https://perma.cc/7EC3-XHYV].

Amendment, intended to constrain arbitrary governmental surveillance, may limit certain uses of facial recognition, but current precedents have established few inarguable or comprehensive limitations.[245] The Supreme Court has not ruled on whether various uses of facial recognition technology by law enforcement violate a person's expectation of privacy such that law enforcement would be required to obtain a warrant before deploying it, though scholars like Andrew Ferguson have asserted that some applications may indeed require one under certain circumstances.[246] Given that people are likely to be unaware of the role facial recognition played in their arrest, and that states do not always require prosecutors to disclose law enforcement use of facial recognition to defendants,[247] people will often be unable to successfully challenge the inadequacy of the evidence used against them. Relevant constitutional protections for individuals, at least as interpreted thus far by the courts, have been manifestly inadequate at protecting people from the harms of facial recognition technologies wielded by law enforcement, and the failure of law enforcement oversight allows the dangerous carelessness with which these systems are deployed from scrutiny.

Shared Harms: Civil Rights Laws

Laws applicable to facial recognitions' quasi-universal harms have been insufficient to prevent, deter, or mitigate them. The failure of laws that could ostensibly prevent that group of harms should alone justify a comprehensive ban, but the use of facial recognition technologies also harms a number of specific demographic groups for whom they are frequently less accurate. Like the laws governing facial recognitions' quasi-universal harms, civil rights laws have also been inadequate to reign in the harms facial recognition inflicts for particular groups by virtue of their race, sex, gender, or age. Also similar to state and federal privacy laws, federal civil rights laws suffer both from being ill-designed to extend to the use of facial recognition technologies, and under-enforced even when they do apply.

A number of federal civil rights statutes do, nevertheless, appear to reach the discriminatory harms inflicted by facial recognition technologies. Title VII of the Civil Rights Act of 1964 prohibits discrimination in employment on the basis of race, color, religion, national origin, or sex,[248] while the Age Discrimination in Employment Act of 1967 prohibits discrimination in employment on the basis

[245] *Facial Recognition Technology Hearings, supra* note 49 (written testimony of Prof. Andrew Guthrie Ferguson).

[246] *Id.* at 9-11; Ferguson, *supra* note 17, at 105 (concluding that legislative intervention is necessary to counteract the Fourth Amendment's relative inability to provide sufficient protections against privacy invasions).

[247] Jennifer Valentino-Devries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan., 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/8M23-TXWG].

[248] 42 U.S.C. § 2000e-2 (2018).

of age:[249] both would apply to the use of facial-recognition-based hiring algorithms. Title VI prohibits discrimination in federally funded programs or activities on the basis of race or national origin,[250] while the Age Discrimination Act of 1975 prohibits discrimination on the basis of age in federally funded programs or activities,[251] both of which would appear to extend to a wide range of use of the technology.[252] Title II of the Civil Rights Act prohibits discrimination on the basis of race in public accommodations, establishments that serve the public in connection to interstate commerce, such as hotels, sports arenas, and the like.[253]

The use of facial recognition systems will almost always be a facially neutral practice, meaning that a plaintiff or regulator would need to be able to demonstrate a disparate impact on a protected class, such as race or gender.[254] But this array of civil rights protections is inadequate to guard against facial recognition's discriminatory harms for a number of reasons—inapt definitions that are unlikely to extend to the use of facial recognition technologies, particularly with the disparate impact standard, federal hostility to civil rights enforcement, and years of the judiciary making access to redress more difficult for plaintiffs.

To start, disparate impact analysis will pose a problem for plaintiffs wishing to demonstrate that the use of facial recognition algorithms in hiring constitutes illegal discrimination under Title VII. In the case of employment, companies like HireVue have incorporated affect analysis into their screening process for job applicants: applicants record themselves responding to interview questions, and HireVue's tool purports to assess attributes like enthusiasm and alertness from physical signals and attributes like language patterns, provided audio cues, and facial expressions.[255] Candidates can be automatically rejected by the software if their scores do not reach a certain threshold, and the potential for discrimination against populations for whom the algorithms are less likely to accurately assess, like women with darker skin,[256] is considerable. But as scholars have noted, the EEOC guidance and related case law are ill-suited to the use of discriminatory machine learning models like Hirevue's.[257] If the outcome of the practice is predictive of future employment outcomes, it can be justified as a

[249] 29 U.S.C. §§ 621-634 (2018).

[250] 42 U.S.C. § 2000d (2018).

[251] 42 U.S.C. §§ 6101-6107 (2018).

[252] Funding recipients cannot "utilize criteria or methods of administration which have the effect of subjecting individuals to discrimination because of their race, color, or national origin." 28 C.F.R. § 42.104(b)(2) (2013); 49 C.F.R. § 21.5(b)(2) (2013).

[253] JODY FEDER, CONG. RESEARCH SERV., RL33386, FEDERAL CIVIL RIGHTS STATUTES: A PRIMER 2 (2012).

[254] *See* Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc., 135 S. Ct. 2507, 2514-15 (2015).

[255] BOGEN & RIEKE, *supra* note 152, at 37.

[256] Buolamwini & Gebru, *supra* note 125.

[257] BOGEN & RIEKE, *supra* note 152, at 11; Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 695-96 (2016).

"business necessity" regardless of whether it reifies or promotes bias based on protected characteristics.[258]

Another area of civil rights law that could plausibly be used to mitigate the harms of facial recognition is the Fair Housing Act. The statute prohibits discrimination against any person in the provision of services or facilities in connection to the sale or rental of a dwelling,[259] which could include the use of a facial recognition system to surveil residents or mandatory facial recognition-contingent locks. The Fair Housing Act also contains a mandate that the federal government and recipients of its funding "administer the programs and activities relating to housing and urban development in a manner affirmatively to further the policies of this subchapter [fair housing]," which could support the argument that installing facial recognition systems in any federally funded housing complex should be prohibited as a violation of that mandate.[260]A 2015 Supreme Court decision confirmed that discriminate impact analysis could be used to demonstrate that discrimination occurred.[261] But the likelihood of actual enforcement is key. The current administration has been deeply hostile to civil rights enforcement[262] and is currently attempting to make it functionally impossible to bring a disparate impact claim under the Fair Housing Act.[263]

Finally, Title II of the Civil Rights Act prohibits discrimination on the basis of race in public accommodations, such as hotels, sports arenas, and the like.[264] Places of public accommodation that deploy facial recognition systems to admit or surveil their customers, like a stadium or department store, could be denying customers of certain demographic groups "full and equal enjoyment of the goods, services, facilities, privileges, advantages, and accommodations" of the establishment.[265] However, Title II only provides for injunctive relief, rather than actual damages, limiting the likelihood of its private enforcement, and does not explicitly include gender or sexual orientation as protected classes.[266] Courts have not yet determined whether plaintiffs may use a disparate impact theory to

[258] Barocas & Selbst, *supra* note 247 at 696; BOGEN & RIEKE, *supra* note 152, at 11.

[259] 42 U.S.C. § 3604(b) (2018).

[260] 42 U.S.C. § 3604(e) (2018); *see also* Olatunde C.A. Johnson, *Beyond the Private Attorney General: Equality Directives in American Law*, 87 N.Y.U. L. REV. 1339, 1364-66 (2018) (discussing the Fair Housing Act's affirmative obligation and arguing for the value of its role).

[261] Tex. Dep't of Hous. and Cmty. Affairs v. Inclusive Cmtys. Project, 135 S. Ct. 2507, 2523-24 (2015).

[262] *The Latest Front Against Civil Rights*, N.Y. TIMES (Jan. 4, 2019), https://www.nytimes.com/2019/01/04/opinion/disparate-impact-discrimination-trump.html [https://perma.cc/3LF2-SKS7].

[263] HUD's Implementation of the Fair Housing Act's Disparate Impact Standard, 84 Fed. Reg. 42854 (proposed Aug. 19, 2019) (to be codified at 24 C.F.R. pt. 100).

[264] 42 U.S.C § 2000a (2018); FEDER, *supra* note 243, at 2.

[265] *See* 42 U.S.C. § 2000a.

[266] Robert B. Duncan & Karl M.F. Lockhart, *The Washington Lawyers' Committee's Fifty-Year Battle for Racial Equality in Places of Public Accommodation*, 62 HOW. L.J. 73, 116, 118 (2018).

demonstrate harm, which is how most plausible claims challenging the use of facial recognition in places of public accommodation would be likely to manifest themselves.[267] Title II, like the other parts of the Civil Rights Act, is an imperfect tool against the broad deployment of facial recognition technologies.

Another practical constraint on the likelihood that federal civil rights laws can successfully mitigate the discriminatory harms of facial recognition is decades of judges making it harder for plaintiffs to sue. Title VI, for example, might appear to offer a broad remedy for victims of discrimination, given how many programs are funded by the federal government—including police departments that receive federal funding.[268] But a 2001 case, *Alexander v. Sandoval*, eliminated a private right of action for its regulations based on disparate impact, meaning that the vast majority of individuals will be unable to bring a case.[269] Enforcement of disparate impact cases, which would be the predominant if not sole makeup of facial recognition cases, is thus left to the federal government—and in this particular case, a federal government that has expressed interest in dismantling disparate impact doctrine rather than using it to vindicate civil rights.[270]

In the case of employment, the EEOC enforces Title VII by investigating charges brought to them by individual employees, and fear of retaliation, expense, and hassle create substantial incentives against potential plaintiffs doing so.[271] Other structural factors, like a 2001 Supreme Court case that makes it harder for private plaintiffs to recover attorney's fees in civil rights litigation, also make private enforcement of civil rights laws more difficult.[272] Enforcement of civil rights laws has been repeatedly and fairly described as under attack by Congress and the courts.[273]

[267] *Id.* at 119.

[268] *See Addressing Police Misconduct Laws Enforced by the Department of Justice*, U.S. DEP'T OF JUSTICE (Dec. 13, 2019), https://www.justice.gov/crt/addressing-police-misconduct-laws-enforced-department-justice [https://perma.cc/K69B-BK35].

[269] Alexander v. Sandoval, 532 U.S. 275, 293 (2001); *see also* Adam Serwer, *Trump is Making it Easier to Get Away with Discrimination*, THE ATLANTIC (Jan. 4, 2019), https://www.theatlantic.com/ideas/archive/2019/01/disparate-impact/579466/ [https://perma.cc/9QCB-KQFA].

[270] Laura Meckler & Devlin Barrett, *Trump Administration Considers Rollback of Anti-Discrimination Rules*, WASH. POST (Jan. 3, 2019, 7:00 AM), https://www.washingtonpost.com/local/education/trump-administration-considers-rollback-of-anti-discrimination-rules/2019/01/02/f96347ea-046d-11e9-b5df-5d3874f1ac36_story.html [https://perma.cc/53M3-PAY7]; *The Latest Front Against Civil Rights*, *supra* note 262.

[271] Heather S. Dixon, *Revisiting Title VII After 50 Years: The Need for Increased Regulatory Oversight of Employers' Personnel Decisions*, 59 HOW. L.J. 441, 450-51 (2016).

[272] Catherine R. Albiston & Laura Beth Nielsen, *The Procedural Attack on Civil Rights: The Empirical Reality of Buckhannon for the Private Attorney General*, 54 UCLA L. REV. 1087, 1092 (2007).

[273] *See* Pamela S. Karlan, *Disarming the Private Attorney General*, 2003 U. ILL. L. REV. 183, 187 (2003); Michael Waterstone, *A New Vision of Public Enforcement*, 92 MINN. L. REV.

The observation that existing civil rights laws are not sufficient to guard against the full range of discriminatory harms inflicted by facial recognition technologies should not be construed as an argument against trying to use them for that purpose. But even where sector-specific arguments might prevail, other discriminatory uses will be left intact, and the combination of the Trump administration's distaste for civil rights enforcement, and the constraints on private enforcement makes the likelihood of success too low to be a reasonable solution. Existing civil rights laws will not be enough to prevent discriminatory harms of facial recognition technologies in the full range of sectors in which they are being deployed.

Child-Specific Harms: COPPA & FERPA

Having discussed the limits of existing laws to mitigate the quasi-universal harms and discriminatory harms inflicted by facial recognition technologies, the question remains: do the relevant child-specific legal protections undermine the need for a facial recognition ban? The answer is unsurprisingly dismal. While the Children's Online Privacy Protection Act, the Family Educational Rights and Privacy Act, and state student privacy laws could be applied to regulate the use of facial recognition technologies on children, they are all either limited in scope, or are currently underenforced to the point that relying on the protections they theoretically confer would be unwise.[274]

The most broadly applicable law, and likely the strongest, is The Children's Online Privacy Protection Act.[275] COPPA governs private companies that collect children's personal information, either through a service specifically directed to children, or when the company has actual knowledge that it is collecting children's information.[276] The statute and accompanying regulations require companies to provide parents with clear notice of their practices, obtain parents' verifiable consent before collecting children's information, allow parents to delete their children's information, and a few other requirements and prohibitions.[277]

COPPA applies to the use of facial recognition technologies on children when companies operating facial recognition programs that constitute an "online service" either direct that service to children, or in the case of a system that collects

434, 443-45 (2007) (describing a "multilevel assault" on the private enforcement of civil rights laws and arguing for a reinvigoration of public enforcement).

[274] *See, e.g.*, *Privacy Bills by State Chart*, PARENT COALITION FOR STUDENT PRIVACY (Jan. 23, 2019), https://www.studentprivacymatters.org/1908-2/ [https://perma.cc/L35P-KACW] (showing that no student privacy law specifically targets facial recognition technology, and none are otherwise sufficiently stringent and applicable enough to force any kind of national limitation on the use of facial recognition technology in general); Waterstone, *supra* note 273, at 443-45.

[275] 15 U.S.C. § 6502 (2012).

[276] *Id.*

[277] *Id.*

images from people in a non-child-specific setting, have actual knowledge that they are collecting facial images from children.[278] A facial recognition system that in any way relies on cloud services, like Amazon's Rekognition, would almost certainly constitute an "online service." Certain programs that might be considered "directed to children" include a daycare monitoring app, a nanny cam, or a service used in a camp or a school.

In the case of general-audience uses of these technologies, companies would need to have actual knowledge that they were collecting information from children.[279] Reasonable judgments can be made from the likely composition of who attends the place under surveillance, like a sports stadium or any other public place where children accompany their parents, and simply using the system—running pictures against an accumulated dataset in order to find a match—would likely provide the company with actual knowledge.[280] So would communications with another party (such as between the facial recognition vendor and the entity deploying the service) that indicated awareness that images of children were being collected, promoting the service as one that would collect pictures of children to potential customers,[281] or automated or manual assessments of images collected that determined the age of the subject.[282] Failing to obtain verifiable consent from parents, not providing them with clear notice, or neglecting to give them an opportunity to review and delete the images, would violate COPPA.[283] So would failing to sufficiently protect the images collected[284] or conditioning the child's participation in an activity, such as attending a summer camp or daycare, upon the collection of pictures of the child's face.[285]

Even to the extent that COPPA applies to certain uses of facial recognition technology, state Attorneys General and the FTC would have to enforce the law more vigorously for it to serve as a meaningful deterrent. Then there are COPPA's other constraints. It only extends to children under 13, leaving 13-year-olds and older teenagers unprotected. The statute lacks a private right of

[278] FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2019).

[279] *See id.* ("A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or on-line service directed to children.").

[280] *See, e.g.*, Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 15, FTC v. Google LLC, No. 1:19-cv-2642 (D.D.C. Sept. 4, 2019) [hereinafter *Youtube Complaint*] ("Defendants gained actual knowledge through, among other things, direct communications with channels owners, their work curating specific content for the YouTube Kids App, and their content ratings.").

[281] *Id.* at 15-16.

[282] *Id.* at 16.

[283] *See* 15 U.S.C. § 6502 (2012).

[284] 16 CFR §312.8 (2019); *see, e.g.* Complaint at 5, United States v. VTech Elecs. Ltd., No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018).

[285] 16 CFR §312.7 (2019).

action, leaving its enforcement the sole province of regulators with strapped resources, competing priorities,[286] and sometimes simply a disinclination to enforce the law.[287] And while fixing these defects would be insufficient to render COPPA a meaningful protection against the use of facial recognition technologies on children, the statute also only applies to companies under the FTC's jurisdiction, and does not extend to law enforcement.

FERPA provides privacy protections that primarily, but not exclusively, cover children, though capacious definitions and exceptions likely make it even less effective to curb the use of facial recognition technologies on young people than COPPA.[288] FERPA generally requires schools to obtain written parental permission before disclosing personal information from students' educational records to third parties, such as if the school disclosed images of students' faces or live footage of them to a company deploying a facial recognition system for the school.[289] While schools cannot require a parent to forfeit their FERPA rights by accepting a tech company's terms of service,[290] the school may not always need to obtain the parent's consent in order to collect images of students' faces and use them in a facial recognition system. A school could designate a third-party contractor as a "school official" with a "legitimate educational interest" in the information,[291] which the school has a worryingly wide latitude to do.[292] FERPA's "Health or Safety" exception also creates the possibility that the school could provide face images to law enforcement in certain circumstances

[286] *See* Reyes et al., *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, DE GRUYTER OPEN: PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES (Mar. 16, 2018), https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf [https://perma.cc/2G34-3NMH] (describing study reporting that the vast majority of Android apps in the Google Play Store directed to children are likely violating COPPA); Federal Trade Commission, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, Comments of Campaign for a Commercial-Free Childhood (Dec. 11, 2019), https://commercialfreechildhood.org/wp-content/uploads/2019/12/CCFC-COPPA-comments.pdf [https://perma.cc/Q446-CCNZ] (criticizing the under-enforcement of COPPA and the incentives it creates for industry).

[287] https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf (criticizing the FTC for failing to enforce COPPA against the most egregious defenders); Nicholas Confessore & Cecilia Kang, Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites, N.Y.T. (Dec. 20, 2018), https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html (describing a cultural reticence at the FTC towards privacy enforcement and citing criticism thereof).

[288] *See* 20 U.S.C. § 1232g (2012); 34 C.F.R. § 99.3 (2019).

[289] 20 U.S.C. § 1232g (2012); 34 C.F.R. § 99.3 (2019).

[290] Letter from Dale King, Director, Family Policy Compliance Office, United States Department of Education, to Agora Cyber Charter School (Nov. 2, 2017), https://studentprivacy.ed.gov/resources/letter-agora-cyber-charter-school [https://perma.cc/9LYX-P6B9].

[291] 34 C.F.R. § 99.31(a)(1) (2019) (providing the "school official" exception).

[292] Maya Weinstein, *School Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 School Security*, 98 N.C. L. REV. 438, 471-3 (2020).

during an emergency, such as a school shooting[293]—precisely the kind of emergency that many schools adopting facial recognition systems have cited as their motivation for doing so.[294] FERPA does not adequately protect children from facial-recognition-fueled surveillance.

COPPA may also provide schools and companies with additional leeway in the educational context. While FERPA is enforced by the Department of Education, companies collecting information from students in schools are also subject to COPPA,[295] and the FTC's guidance for distinguishing when schools may provide consent on behalf of parents may provide schools with sufficient legal cover. The FTC states that companies collecting information from children under 13 in schools may obtain consent from schools, rather than parents, when information is for the use and benefit of the school, and no commercial purpose.[296] However, the FTC provides little guidance over what purposes are "educational" or "commercial," and a school (or company) could argue that the use of a facial recognition system for security purposes fits the educational designation. Moreover, as noted above, schools do not have to obtain written permission when disclosing student personal information to a "school official serving a legitimate educational interest," and schools and education tech companies have previously relied on the exception to avoid having to obtain parental consent.[297]

More fundamentally, FERPA is even more rarely enforced than COPPA.[298] While a school can lose its funding for a "policy or practice" of violations (not a single violation), no school ever has in the 45-year-history of the statute.[299] FERPA also lacks a private right of action, such that its enforcement is solely determined by regulators.[300] Even if FERPA were a better fit for the kinds of concerns that facial recognition technologies present, its relevance unfortunately

[293] *Protecting Student Privacy*, U.S. DEP'T OF EDUC. (2020), https://studentprivacy.ed.gov/faq/when-it-permissible-utilize-ferpa%E2%80%99s-health-or-safety-emergency-exception-disclosures [https://perma.cc/B5EC-MVKB].

[294] Rebecca Heilweil, *Schools Are Using Facial Recognition to Try to Stop Shootings. Here's Why They Should Think Twice.*, VOX (Dec. 20, 2019, 10:00AM), https://www.vox.com/recode/2019/12/20/21028124/schools-facial-recognition-mass-shootings [https://perma.cc/9EBT-P3UA].

[295] *See* 15 U.S.C. § 6501 (2012).

[296] 34 C.F.R. § 99.31 (2019).

[297] Federal Trade Comm'n, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, Comments of Campaign for a Commercial-Free Childhood (Dec. 11, 2019), https://commercialfreechildhood.org/wp-content/uploads/2019/12/CCFC-COPPA-comments.pdf [https://perma.cc/Q446-CCNZ] (criticizing the breadth of the school official exception and the breadth of privacy violations it permits).

[298] 20 U.S.C. § 1232g (2012); 34 C.F.R. § 99.1 (2019).

[299] *See* Elana Zeide, *The Limits of Education Purpose Limitations*, 71 U. MIAMI L. REV. 494, 503 (2017).

[300] Gonzaga University v. John Doe, 536 U.S. 273, 273 (2002).

depends on regulators deciding to do what they have never done as long as the law has been in existence.

CHILDREN'S VULNERABILITY TO FACIAL RECOGNITION SUPPORTS A COMPREHENSIVE BAN

As this article attempts to illustrate, existing legal protections that should extend to the use of facial recognition technologies are sorely insufficient to curb their use, the harms created by these technologies are widespread and severe, and they have grave implications for fundamental freedoms when used by law enforcement or by private entities. Not only is a comprehensive ban on these technologies necessary, but the harms that children experience provide an additional argument for it: young people need to be protected from invasive surveillance, chilled expression, and the dangers of errors. Further, few of the harms to children are entirely unique to them, and eradicating only those harms would be an inadequate response to facial recognition technologies' far-reaching damage to democratic values. The severe harms to children further support a ban on the use of facial recognition technologies, but the harms to adults alone justify and necessitate it.

The Need for a Comprehensive Ban

Facial recognition technologies should be banned because they corrode privacy and due process, damage free expression, and enable dangerous discrimination, all while being difficult or impossible to avoid. Consensus has started to coalesce around the idea of regulating certain uses of facial recognition technologies, and calls for regulation have become so widespread that even the companies selling them have joined the throng.[301] Current proposals range from procedural rules for commercial uses,[302] procedural rules for law enforcement uses,[303] a moratorium on its deployment in "sensitive social and political contexts,"[304] a

[301] *See, e.g.*, Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, MICROSOFT ON THE ISSUES (Jul. 13, 2018), https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/ [https://perma.cc/UUF7-7PMD]; Madeline Purdue, *Axon Body-Camera Supplier Will Not Use Facial Recognition in its Products – For Now,* USA TODAY (July 1, 2019, 2:17 PM), https://www.usatoday.com/story/tech/2019/07/01/axon-rejects-facial-recognition-software-body-cameras-now/1601789001/ [https://perma.cc/F24Z-M5T7].

[302] *See* Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. § 1 (2019).

[303] *See* Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. § 1 (2019).

[304] Kate Crawford et al., *AI Now 2019 Report*, NEW YORK: AI NOW INSTITUTE, at 6 (2019), https://ainowinstitute.org/AI_Now_2019_Report.html [https://perma.cc/2ZJX-56DA].

comprehensive moratorium,[305] a ban on certain uses by law enforcement,[306] a ban on all uses by law enforcement,[307] a ban on deployment in public housing,[308] a ban on emotional affect detection,[309] and a comprehensive ban on all uses.[310] More recently, the nationwide reckoning with racist police violence following the brutal killing of George Floyd seems to have leant additional urgency to the growing criticism of use of these technologies by law enforcement. IBM announced it would no longer offer "general purpose" facial recognition products, Microsoft announced it would not offer its services to law enforcement until there was an applicable federal law "grounded in human rights," while Amazon announced a one-year moratorium on police use of Rekognition.[311] The tides are shifting, and they're shifting quickly.

[305] Letter from the ACLU et al., to The Honorable Elijah Cummings et al., Chairman, U.S. House Oversight and Reform Committee, (June 3, 2019) (on file with ACLU).

[306] Friedman & Ferguson, *supra* note 13; Rachel Metz, *California lawmakers ban facial-recognition software from police body cams*, CNN (Sept. 13, 2019), https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html [https://perma.cc/V4KR-FHHP] (ban on body cams).

[307] Shirin Ghaffary, *Bernie Sanders wants to ban police use of facial recognition technology,* VOX (Aug. 10, 2019) https://www.vox.com/recode/2019/8/19/20812594/bernie-sanders-ban-facial-recognition-tech-police [https://perma.cc/9DW7-LW8M]; *Facial Recognition Technology Hearings, supra* note 49, at 25 (written testimony of Prof. Andrew Guthrie Ferguson); Sigal Samuel, *Facial recognition tech is a problem. Here's how the Democratic candidates plan to tackle it.*, VOX (Sept. 12, 2019), https://www.vox.com/future-perfect/2019/8/21/20814153/facial-recognition-ban-bernie-sanders-elizabeth-warren-kamala-harris-julian-castro-cory-booker [https://perma.cc/YQ3P-VKUP]; Candice Bernd, *States, 2020 Candidates Push Back Against Facial Recognition Technology*, Truthout (Sept. 24, 2019), https://truthout.org/articles/states-2020-candidates-push-back-against-facial-recognition-technology/ [https://perma.cc/64W8-5RMW]).

[308] Press Release, Corey Booker, Booker Introduces Bill Banning Facial Recognition Technology in Public Housing (Nov. 1, 2019), https://www.booker.senate.gov/?p=press_release&id=1007 [https://perma.cc/MWZ6-F4ZT].

[309] Crawford et al., *supra* note 304, at 6.

[310] Evan Selinger et al., *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html [https://perma.cc/4CLM-8PJC]; Hartzog, *supra* note 14; BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/ [https://perma.cc/ZK3D-VNCY].

[311] Lindsey Barrett, *A Pause on Amazon's Police Partnerships is Not Enough*, SLATE (June 12, 2020, 2:31 PM), https://slate.com/technology/2020/06/amazon-rekognition-law-enforcement-moratorium.html [https://perma.cc/X822-ZALQ].

The idea of banning facial recognition outright has also grown more popular in the past few years, particularly with states and municipalities. San Francisco,[312] Somerville,[313] Boston,[314] Oakland,[315] and Berkeley[316] have banned the use of facial recognition technology by city government, including but not limited to law enforcement. A two-year moratorium on the use of facial recognition technology in New York schools passed both houses of the state legislature and awaits the governor's signature.[317] California recently passed a three-year ban on law enforcement uses of facial recognition in body cameras,[318] and a proposed ordinance in Portland, Oregon would ban the use of facial recognition by both law enforcement and private businesses.[319] A California legislator announced plans to introduce a bill that would ban government uses of facial recognition for the next five years, while Senators Booker and Merkley introduced a bill that would ban federal uses of the technology and prohibit states and

[312] Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/3YM0-EQGR].

[313] *Somerville Becomes First East Coast City to Ban Government Use of Face Recognition Technology*, ACLU (June 28, 2019), https://www.aclu.org/press-releases/somerville-becomes-first-east-coast-city-ban-government-use-face-recognition [https://perma.cc/J4YH-V8HS].

[314] Ally Jarmanning, *Boston Lawmakers Vote to Ban Use of Facial Recognition Technology by the City*, NPR (June 24, 2020, 7:05 PM), https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city [https://perma.cc/M3GA-F6CD].

[315] *Oakland Approves Face Recognition Surveillance Ban as Congress Moves to Require Government Technology*, ACLU (July 17, 2019), https://www.aclu.org/press-releases/oakland-approves-face-recognition-surveillance-ban-congress-moves-require-government [https://perma.cc/46B9-SS28].

[316] Tom McKay, *Berkeley Becomes Fourth U.S. City to Ban Face Recognition in Unanimous Vote*, POPULAR RESISTANCE (Oct. 18, 2019), https://popularresistance.org/berkeley-becomes-fourth-u-s-city-to-ban-face-recognition-in-unanimous-vote/ [https://perma.cc/A258-YFGM].

[317] Connor Hoffman, *Facial Recognition moratorium passes state senate*, LOCKPORT UNION-SUN & J. (July 22, 2020), https://www.lockportjournal.com/news/local_news/facial-recognition-moratorium-passes-state-senate/article_f617ee40-cc5f-11ea-939e-0785f62d0f92.html [https://perma.cc/X3WE-XE36].

[318] Katy Stegall, *3-year ban on police use of facial recognition technology in California to start in the new year*, The San Diego Union Tribune (Dec. 20, 2019), https://www.sandiegouniontribune.com/news/public-safety/story/2019-12-20/3-year-ban-on-police-use-of-facial-recognition-technology-in-california-to-start-in-the-new-year [https://perma.cc/UF2P-MBCT]; Matthew Guariglia, *Victory! California Governing Signs A.B. 1215* (Oct. 9, 2019), https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215 [https://perma.cc/W7CQ-LLFL].

[319] Sean Captain, *Portland plans to propose the strictest facial recognition ban in the country*, FAST COMPANY (Dec. 02, 2019), https://www.fastcompany.com/90436355/portlands-proposed-facial-recognition-ban-could-be-the-strictest-yet [https://perma.cc/H23W-YVVP].

local entities from using federal funding for it until Congress passes legislation regulating it.[320] The goal of a comprehensive and federal ban on facial recognition may be lofty, but it is not impossible given the enormous shift in awareness and political will.

Enacting procedural rules rather than banning facial recognition is, of course, preferable to no regulation at all. But the very goal of regulation assumes that there is value to the use of these technologies that outweighs the harms they wreak. The scale, severity, and variety of harms in question, along with the limited value of the benefits, belie that conclusion. Procedural protections like notice and opt-out rights are unlikely to sufficiently curb the full breadth of harms imposed by these technologies, just as they are insufficient to curb other privacy harms.[321] The likelihood of mission creep[322] is also far too great. Procedural regulation is a suitable approach to conduct that has socially valuable benefits worth preserving, and social dangers that are minimal or unlikely enough that the risk of an insufficient regulatory response is tolerable. That is not the case with facial recognition technologies.[323]

Julie Cohen's[324] and Ari Waldman's[325] critiques of the "managerialization" of privacy law help demonstrate why procedural rules would be inadequate. As they describe it, the shift of authority over what privacy regulations practically mean from judges and regulators to corporate compliance officers has reduced the substantive goals of statutory privacy protections to hollow, symbolic box-checking exercises. This shift, exacerbated by the proliferation of ambiguous standards that necessitate interpretation by corporate compliance officers, has

[320] *Jackson Announces a Ban on Facial Recognition Technology*, CAL. SENATE DISTRICT 19 (Feb. 13, 2020), https://sd19.senate.ca.gov/news/2020-02-13-jackson-announces-ban-facial-recognition-technology [https://perma.cc/7NLS-2Y4P]; Ethical Use of Facial Recognition Act of 2020, S.3284 116th Cong. § 2 (2020) (the Booker and Merkeley proposal would permit the use of facial recognition technology by law enforcement with a probable-cause warrant).

[321] See Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1880, 1881 (2013).

[322] *See, e.g.*, Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101, 102 (2019); Bruce Schneier, *NSA Surveillance and Mission Creep*, SCHNEIER ON SECURITY (Aug. 6, 2013, 6:16 AM), https://www.schneier.com/blog/archives/2013/08/nsa_surveillanc.html [https://perma.cc/KJ9W-FCXS].

[323] *See* Selinger & Hartzog, *supra* note 322, at 105 ("Building an infrastructure to facilitate surveillance will also provide more vectors for abuse and careless errors. . . . Procedural rules wouldn't address the true harm of these technologies without further prohibitions to prevent end-runs around the aims of a restriction. . . . In all areas where consentability conditions cannot be met, and procedural rules and compliance frameworks for government and industry will facilitate an outsized harm and abuse relative to their gains, facial recognition technology should be outright banned.").

[324] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 143-47 (2019).

[325] Ari E. Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 1, 4-8 (2020).

diluted the substantive goals of privacy laws from providing what is necessary to ensure privacy rights are respected to providing what is sufficient to avert expensive fines.[326] In the case of facial recognition technologies, the most likely outcome is that companies will push the boundaries of profitable products and services that fail to meaningfully protect people from any number of harms.

Privacy policies and check-the-box compliance exercises will not be sufficient to constrain the dangers of facial recognition technologies, particularly given the lack of vigorous regulatory oversight and the difficulty that privacy litigants face in the courts— that is, when the victims of privacy violations even have a private right of action that will supply them with a judicial forum.[327] The benefits of facial recognition technologies are far too minimal and the harms far too great to accept what Waldman describes as "a neoliberal ethos that prioritizes deregulated markets and corporate innovation over human welfare."[328]

The idea of a temporary moratorium on the technology is preferable to leaky procedural rules, but tends to rest on the idea that there will ever be a time when they work equally well for all demographic groups, which may never be possible.[329] Even in a magical world where the full range of bias problems were capable of correction, the end date of the moratorium would mean that the harms to privacy, free expression, and due process would return. Bans limited to law enforcement uses of facial recognition technologies are an excellent start, but are still insufficient given how porous the line between law enforcement and private uses often is, and the dangers of commercial uses.[330] Mission creep is far

[326] *Id.* at 18-19, 37-38, 62 ("[Some privacy professionals] see privacy as one part of a compliance ecosystem focused on enhancing efficiency, speed, and productivity, while reducing the risk of debilitating fines…although consumers can benefit when companies start thinking about privacy as good for business, the value proposition is nevertheless shifted from what helps consumers to what helps corporations. When that happens, those responsible for compliance advance managerial, rather than substantive, privacy goals…merely symbolic structures are often being used to advance management goals to the detriment of consumers. . . Privacy law is at risk… it is undergoing a process of what Lauren Edelman called legal endogeneity, whereby systems that have the veneer of legality—paper trails, assessments and audits, internal and external policies, to name just a few—take the place of actual adherence to the law. And when these merely symbolic structures proliferate, they undermine the substantive power of the law and shift the discourse of power, all to the detriment of consumer privacy.").

[327] *Id.* at 58-9; Cohen, *supra* note 194, at 535-36 (describing the track records of private litigation in vindicating privacy harms as "stunningly poor" as the result of "denial of standing, enforcement of boilerplate waivers, denial of class certification, disposal via opaque multidistrict litigation proceedings, and cy pres settlements.").

[328] *Id.* at 49.

[329] BOGEN & RIEKE, *supra* note 148.

[330] *"Artificial Intelligence: Social and Ethical Implications": Hearing Before the H. Comm. On Science, Space and Tech.,* 116th Cong. 10-12 (2019) (written testimony of Meredith Whittaker, Co-founder and Co-director, AI Now Inst. NYU).

too likely and difficult to prevent,[331] and abuse under opaque standards is a significant contributing factor to how these technologies currently put democratic values, like due process rights, at risk. For a class of services with severe bias problems designed with the explicit objective of making anonymity impossible, a comprehensive ban is the most appropriate response. The harms are vast and far-reaching; the response must be also.

A Child-Specific Ban is Not Sufficient, Defensible, Or Feasible

Many of the harms that are either broadly shared or shared by some demographic groups may have particularly severe consequences for children, like the potential chilling effects of surveillance on their emotional and intellectual development early on, or early exposure to the criminal justice system through inclusion in a law enforcement database. The harms that facial recognition surveillance creates may have an outsized impact on the lives of young people by virtue of the fact that their anonymity is eroded earlier in their lives, and the ramifications of any kinds of fairness implications will affect them at a time when they're more vulnerable.[332]

That vulnerability to facial recognition technologies merits strong privacy protections, but there is no defensible basis for stronger civil liberties protections for one demographic group that is vulnerable to discrimination through the use of the technology by virtue of who they are, but not the other groups who are similarly vulnerable. Some of the harms children experience are uniquely severe for them, but relativity is key: the harms that facial recognition technologies inflict on all groups merit a ban even without the additional severity of the harms to children. Studies have shown that facial recognition algorithms are less accurate for children's faces, but as discussed above, those studies have also shown the failure of those algorithms to accurately assess the faces of Asian people, Black people, women, and the elderly—and many aren't even designed to account for the existence of non-binary or trans people at all. The potential for discrimination extends to those groups as well, and while the forms of discrimination may vary, they are all concerning enough to warrant intervention.

Further, certain use cases and vulnerabilities for children as compared to other groups simply aren't comparable in a meaningful way such that a child-limited prohibition would be defensible. Children are subject to disproportionate surveillance beyond their control given the concerns of adults for their safety, and they often have limited autonomy over their movements. The same is true for the disproportionate surveillance of residents of public housing—which, of

[331] Ryan Mac et al., *supra* note 164 (Consider, for example, how Clearview AI assured reporters that it only sold its service to law enforcement, while urging law enforcement to try out their technology "on family and friends.").

[332] *See* Valerie Steeves & Owain Jones, *Surveillance, Children and Childhood*, 7 SURVEILLANCE AND SOCIETY at 2 (2010) ("The pervasiveness of the adult gaze and adult ordering of the world and children's lives, even to the extent of the surveillance and ordering of children's very bodies (James 2000), should not be underestimated.")

course, includes children and teenagers—whose ability to protect or reject unwanted surveillance is often limited.[333] Children surveilled in schools and adults in public housing often do not have a meaningful way to avoid face surveillance, and the privacy and freedom of the latter group should be protected just as much as the privacy and freedom of the former.

Children's incapacity to consent to surveillance is another factor that makes it a particularly unfair intrusion into their private lives. But ultimately, children and adults alike have little control over whether facial recognition technologies are used on them.[334] Many of the most problematic uses occur without the surveiller even attempting to obtain consent, and when consent is obtained from adults, it is almost always uninformed, if not flatly coerced. Consent to Facebook's terms of service is not a meaningful indication of knowing acceptance when the company permits a facial recognition service to scrape its platform and build tools for commercial[335] or law enforcement use.[336] Consent is not a meaningful protection against government-collected images like driver's license photos or visa from being repurposed for facial recognition databases—people need to be able to drive cars and travel. A robust literature also illustrates just how poorly adults are situated to make informed privacy decisions, given the complexity and length of privacy policies and the frequency with which people encounter them.[337] As much as children and teens struggle to accurately assess privacy risks, so too do adults. Children being exploited in a slightly more egregious way does not justify the exploitation of everyone else.

Beyond the lack of normative merits, a child-specific ban would also be exceedingly difficult to coherently design and effectively enforce. COPPA attempts to strike the balance of limiting data collected from children without unduly limiting the collection practices of general audience services through a two-pronged applicability approach: the statute applies to companies that direct services to children and companies that do not deliberately target them, but do have actual knowledge that they are collecting personal information from children

[333] Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html [https://perma.cc/YGJ7-WJA2].

[334] *See* discussion *supra* Sections II.ii-iii.

[335] Ng, *supra* note 4.

[336] Hill, *supra* note 51.

[337] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1887 (2013) ("People have 'bounded rationality' — they struggle to apply their knowledge to complex situations — with regard to privacy. . . 'our innate bounded rationality limits our ability to acquire, memorize, and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics' . . . Risk assessment is also skewed by the 'availability heuristic,' where people assess familiar dangers as riskier than unfamiliar ones."); Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. (forthcoming 2020) (detailing the cognitive and structural constraints on individual privacy decision-making and arguing for privacy laws based on restraining corporate practices rather than individual privacy choices).

anyway. The results have been murky at best. The high bar of an actual knowledge standard has allowed general audience services to feign ignorance of the children on their platform, while the lack of enforcement has incentivized companies to ignore it, given that failing to comply with COPPA is unlikely to produce an investigation or penalty.[338] The harms that these technologies inflict on adults are too significant for an intervention that deliberately excludes them to be desirable or sufficient. But even if the harms to adults could be defensibly ignored, attempting to distinguish child-specific from general uses will be unreliable and under-inclusive. A facial recognition law should not replicate COPPA's mistakes, it should learn from them by simply setting a higher standard for everyone.

Moreover, as this article has attempted to illustrate, the harms that are particularly heightened for children are still severe for adults, with the same result of eroding their privacy, free expression, and due process rights. Knowledge of surveillance may have particular implications for children's intellectual development and political freedom, but it also chills free expression for adults. Facial recognition technology's singularly pernicious assortment of attributes as a surveillance tool—that hiding or changing your face is impracticable or impossible, that it weaponizes existing databases of photographs, and consent is often ill-informed and coercive on the rare occasions it's even sought—generally implicates all age groups. Having a picture or video of you used in a facial recognition search by law enforcement is more likely to result in an erroneous result for certain groups, but law enforcement's surreptitious use of these technologies in investigations still affects due process rights for everyone. A child-specific ban would not address any of these dangers, and would thus be an overly narrow response to a far broader problem.

Finally, child-specific privacy protections can still be an acceptable or even welcome policy approach in other circumstances where they are necessary for children, and inapplicable to adults. A regulatory regime that provided strong, comprehensive privacy protections for all people, with meaningful enforcement by the government and private plaintiffs and functional redress for violations, might invite additional, heightened protections for children in situations that

[338] FED. TRADE COMM'N, REQUEST FOR PUBLIC COMMENT ON THE FEDERAL TRADE COMMISSION'S IMPLEMENTATION OF THE CHILDREN'S ONLINE PRIVACY PROTECTION RULE 1 (Dec. 11, 2019), https://commercialfreechildhood.org/wp-content/uploads/2019/12/CCFC-COPPA-comments.pdf [https://perma.cc/7XSM-H9S5] (criticizing COPPA's under-enforcement and the perverse incentives it creates for industry); Craig Timberg, *Sex, Drugs, and Self-Harm: Where 20 Years of Child Online Protection Law Went Wrong*, WASH. POST (June 13, 2019, 8:00 AM), https://www.washingtonpost.com/technology/2019/06/13/sex-drugs-self-harm-where-years-child-online-protection-law-went-wrong/ [https://perma.cc/F6PF-6E46] ("But the legislation's sponsors, who negotiated against powerful industry interests while seeking support in Congress, agreed to a key loophole: So long as online sites didn't explicitly target children and didn't have "actual knowledge" that a particular user was younger than 13, COPPA's restrictions didn't apply.").

generally don't exist for adults, such as privacy in school settings, or even privacy protections for children from their parents.[339] Nor am I arguing that COPPA should be wholly preempted by a general facial recognition technology ban, given the valuable, if highly imperfect, protections COPPA provides for children in contexts beyond the use of facial recognition technology. But in the context of technology or circumstances that implicate both children and adults, the heightened vulnerability of children should not invite the assumption that protections for adults are not similarly needed. In the case of facial recognition technologies, children's autonomy, safety, and freedom are not *uniquely* under threat such that protections for them alone are necessary, and protections for adults are unnecessary. On the contrary.

FURTHER CONSIDERATIONS

An argument for banning facial recognition technologies because of the range of harms they inflict would be incomplete without at least a brief discussion of the technologies' perceived benefits. Proponents of commercial applications of facial recognition tend to highlight the convenience of using one's face as a biometric identifier.[340] People struggle to remember complex passwords and simple ones are easy for hackers to crack, whereas, proponents argue, a face is unique and diminishes the possibility of human fallibility creating a security vulnerability at that particular vector.[341] But the benefits of the identifier hinge on its accuracy, which, as this article has attempts to explain, varies starkly among demographic groups. A definition of "convenience" that excludes young people, older people, women, people with darker skin, Asian people, and gender nonbinary people does not mean much. Moreover, the very fact that a face is a functionally irreplaceable identifier makes the security implications all the more severe when databases are hacked.

[339] *See* Louise Matsakis, *On TikTok, Teens Meme the Safety App Ruining Their Social Lives*, WIRED (July 12, 2019, 7:00 AM), https://www.wired.com/story/life360-location-tracking-families/ [https://perma.cc/R62N-3TBB]; Abby Ohlheiser, *'Don't leave campus', Parents are now using tracking apps to watch their kids at college*, WASH. POST (Oct. 22, 2019, 7:00 AM), https://www.washingtonpost.com/technology/2019/10/22/dont-leave-campus-parents-are-now-using-tracking-apps-watch-their-kids-college/ [https://perma.cc/8QP2-PBDQ]; Brett Singer, *11 Best Apps for Parents to Monitor Their Kids*, PARENTS (June 11, 2020), https://www.parents.com/parenting/technology/best-apps-for-paranoid-parents/ [https://perma.cc/6RZ5-EUAF].

[340] Brief for Internet Association as Amicus Curiae Supporting Appellant at 12, Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019) (No. 18-15982); Simonite & Barber, *supra* note 65; Dan Maunder, *How Brands are Saving Face: Five Ways Facial Recognition is Improving Our Lives*, IT PROPORTAL (May 10, 2018), https://www.itproportal.com/features/how-brands-are-saving-face-five-ways-facial-recognition-is-improving-our-lives/ [https://perma.cc/PN9M-LXHC].

[341] David Harding, *Facial Recognition: When Convenience and Privacy Collide*, SECURITY MAG. (July 22, 2019), https://www.securitymagazine.com/articles/90533-facial-recognition-when-convenience-and-privacy-collide [https://perma.cc/HZ8Z-8T3X].

Perhaps the most fervently touted argument for the value of facial recognition technologies is their purported utility in law enforcement and national security contexts.[342] "The ability to more easily identify criminals makes us all safer" is a temptingly simple argument. But as even many law enforcement professionals have argued,[343] technology that is less accurate for a wide range of demographic groups does not bolster collective safety, it diminishes it by subjecting members of those groups to unwarranted scrutiny and directing officers to pursue erroneous leads. As discussed above, reports of shoddy data practices abound, even despite a lack of transparency surrounding police uses of these technologies.[344] Little evidence exists to support the notion that facial recognition technologies actually enable police officers to do their jobs better by helping them to correctly identify suspects. In fact, evidence that it does the opposite only continues to mount.[345]

Ultimately, most of the claims concerning the benefits of facial recognition technologies are false, like the safety narrative, while others are simply not sufficient to outweigh the severe costs to privacy, due process, and free expression. Technology that subjects people of color to even more disproportionate police scrutiny imperils their freedom and safety, rather than bolstering it. The ability to identify protestors doesn't make anyone safer, it gives the government license to chill free expression and quash dissent. Subjecting children to surveillance in schools is unlikely to prevent a school shooting, as even some vendors admit.[346] Facial recognition databases used by either government or law enforcement also

[342] DEP'T OF JUSTICE, THE USE OF FACIAL RECOGNITION TECHNOLOGY BY GOVERNMENT ENTITIES AND THE NEED FOR OVERSIGHT OF GOVERNMENT USE OF THIS TECHNOLOGY UPON CIVILIANS (June 4, 2019), https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Wstate-DelGrecoK-20190604.pdf [https://perma.cc/97NA-82R5]; Event Summary, Info. Tech. & Innovation Found., The Value of Facial Recognition in Law Enforcement (July 24, 2019), https://itif.org/events/2019/07/24/value-facial-recognition-law-enforcement [https://perma.cc/XJU4-JZ9J]; James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/37J9-E26F]; Ashley Deeks & Shannon Togawa Mercer, *Facial Recognition Software: Costs and Benefits*, LAWFARE (Mar. 27, 2018, 9:00 AM), https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits [https://perma.cc/7ZJU-QLJX].

[343] *Facial Recognition Technology Hearings, supra* note 49, at 1 (opening Statement of Dr. Cedric Alexander).

[344] *Id.* at 12-16 (testimony of Clare Garvie)

[345] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where it Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/KN5Q-DJ4Y]; Pangburn, *supra* note 244.

[346] Alfred Ng, *Facial Recognition in Schools: Even Supporters Say It Won't Stop Shootings*, CNET (Jan. 24, 2020, 5:00 AM), https://www.cnet.com/features/facial-recognition-in-schools-even-supporters-say-it-wont-stop-shootings/ [https://perma.cc/F6XD-5ZGN].

create new sources of hackable information that leave people vulnerable to identity theft and fraud. Despite the rhetoric of its defenders, facial recognition technologies imperil the people and values they purportedly protect.

CONCLUSION

The use of facial recognition technologies on children endangers their well-being despite the fact that their surveillance is often intended for their protection. The developmental immaturity of young people means that the chilling effects of surveillance may be particularly impactful on their emotional and intellectual growth, and arbitrary errors in law enforcement investigations may have particularly severe consequences for their safety, freedom, and life trajectories. But even the harms that are uniquely severe for children are still severely felt by the other demographic groups for whom facial recognition technologies tend to perform poorly, and the damage that these services wreak on privacy, free expression, and due process is essentially universal. Children should be protected from the destructive effects of facial recognition technologies, so should everyone else, and the harms that are even more severe for children are damaging enough for adults alone to necessitate a ban.

The range of proposals for how to regulate facial recognition is wide, but the existence of those proposals and the success of local bans and moratoria are significant reasons for optimism. A comprehensive ban at the federal level is a lofty goal, to be sure— but the limits of the more modest solutions illustrate why a comprehensive ban is worth striving for. A regulatory scheme that permits the use of facial recognition technologies on the basis that enforcement of violations will be enough to deter and prevent undesirable behavior will be inadequate, and ignores how privacy law can be co-opted in to procedural symbolism,[347] how privacy plaintiffs struggle to receive judicial redress,[348] and the inertia of privacy regulators. Moratoria, while a far superior option over regulation, assume a point in time where facial recognition technologies will be sufficiently free of bias—a moment that may never come. Bans on law enforcement uses correctly recognize the particular danger of police use of these surveillance technologies. But private uses can fuel law enforcement ones, and the privacy, free expression, and discrimination concerns are all considerable given the size of the role that private companies play in American lives.

Facial recognition technologies threaten fundamental democratic values that should be fulsomely protected for everyone. A bleak future of inescapable, dragnet surveillance is not only not inevitable, but surmountable, by prohibiting the use of the technology hastening it.

[347] Waldman, *supra* note 325, at 776-77; Cohen, *supra* note 203, at 537-38, 575, 578.

[348] Waldman, *supra* note 325, at 831-32; Brookman, *supra* note 204, at 365.