Facial Recognition Technology

A Primer

#FairTech Series: Race, Social Justice and Technology

Access Partnership

Foreword

At Access Partnership, we recognize the importance of balancing the interests of consumers, citizens, and governments with enabling sustainable market access for technology leaders. We call it "Fair Tech."

In that regard, we respectfully present the first in what we hope is a series of primers examining technologies and their impact on society. Inspired by the non-partisan work of the Congressional Research Service, this edition focuses on facial recognition and its impact on race, social justice, diversity and inclusion, noting the challenges faced when deploying technologies that can be problematic in their use. Topics planned for future reports in the series include "AI and Predictive Policing" and "Social Media and Hate Speech."

The purpose of this series to inform and equip policy professionals who may be brought into top-level conversations or newly established committees dedicated to issues such as race, diversity and inclusion. And government affairs teams have a crucial role to play as an indispensable liaison between the state and corporate leadership.

Access Partnership is positioned to assist companies grappling with these very real and very important issues. Thank you for reading.

Kathryn Martin
Director, Asia & US

Contents

Executive Takeaways

- Police use of facial recognition technology has scaled significantly in recent years. This technology has long utilized an array of public sector resources facial image data sets, while off-the-shelf private solutions using publicly gathered datasets are increasingly available and used.
- While law enforcement asserts this is a key tool to ease their work, critics point to a lack of transparency in the technology's use, systematic inaccuracies, due process questions, and invasion of privacy. Instances of targeting of individuals in specific communities or exercising certain speech rights risks a dangerous unbalancing of the state/citizen relationship.
- Studies on the performance of facial recognition point to systematic errors in identification, especially prevalent for persons of color, which create harms that reinforce disproportionate policing of individuals and ethnic groups of color.
- Policy-makers and stakeholders have put forward many different solutions to mitigate racial inequities. At a technical level, these may target sources of bias in the operation of the technology. However many also prohibit or place obstacles before its use by law enforcement, or create new legal safeguards on when and how the technology can be used.
- While many in law enforcement seek to facilitate continued deployment of facial recognition, an array of stakeholders from diverse perspectives – including both left and right voices in Congress and civil society, rights advocates, and tech companies – have coalesced around implementing temporary or permanent bans on uses of facial recognition technology.
- Several tech companies have voluntarily sacrificed revenue to control blowback from harmful deployments of facial recognition technology. However, unless a more permanent regulatory solution is developed, this voluntary restraint may evaporate.

What Went Wrong?

In June 2020, as mass protests were sparked by the killing of George Floyd at the hands of an officer of the Minneapolis Police Department, several major tech companies took surprising action. In quick succession, IBM, Amazon, and Microsoft, among others, all announced that they would voluntarily pause or turn away from selling facial recognition technology, particularly to police departments.[1] While this was a small sacrifice for Microsoft, which claims to have never sold facial recognition to law enforcement, Amazon was halting actual services provided to public agencies across the United States, while IBM was forfeiting its entire line of business in this area, for both public and private customers.

Although an extraordinary development, concerns regarding police use of facial recognition had been growing for years, placing pressure on these companies. Amazon had been asked by advocacy groups since at least 2018 to halt sales to law enforcement,[2] while Microsoft had long campaigned for regulation of facial recognition. As increasing studies revealed systematic bias, and accounts of abuse came to light, concerns around mass surveillance, racial profiling, and discriminatory impacts – especially in light of the Black Lives Matter protests – became too much for the companies to tolerate. Amid a general reckoning around race, these companies judged that the long-term and short-term costs of continuing the status quo, both public and political, outweighed the returns on investment.

As these same companies and many others now push for more aggressive regulatory action to mitigate harms from uses of facial recognition, and rebuild trust in these products, this situation stands as a cautionary tale of how social challenges, legal systems, new technology development and commercial pressures collide around racial justice and the use of technology by law enforcement.

What Is the Technology?

Facial recognition refers to using computer algorithms that identify features of a person's face in order to match an anonymous photo to that of a person whose identify is known. It differs from "facial detection" common among augmented reality platforms, like Snap or FaceTime, utilized to detect the presence of a face, without analyzing its attributing features leading to recognition.

Using either still images or video inputs, facial recognition systems generally seek to match distinguishing patterns of a person's face, often referred to as the digital template, against a database of records. Such systems can return multiple potential matches or calculate a probability score that an identification is correct. Leveraging training data sets, technology companies develop and train algorithms skilled at identifying these patterns, which are then deployed by the user: in this case, law enforcement.

Law enforcement agencies in the United States and elsewhere have utilized facial recognition technology in various forms for nearly 20 years, to identify suspects based on pictures when the identification could not otherwise be made. However, the practices of law enforcement, the capabilities of the underlying technology and the commercial environment have evolved over time. Facial recognition systems vary by capability and accuracy, presentation of outputs, the way the database is queried, as well as data sources drawn upon. Generally, there are a few different types of facial recognition tools used by law enforcement today:

- **Public sector databases** – a long-used technique based on inputting a still image to query a pool of facial images collected by different government agencies. While the technology is generally provided by the public sector, they are contracted by, gather their data from, and are available to public sector entities.

- **Private databases** - a more recent innovation based on inputting a still image to query a dataset compiled of images publicly available or accessible over the Internet. Developed by private sector actors, they are licensable, in theory, to any entity.

- **Real-time identification** - increasingly, law enforcement has access to technologies that allow them to identify individuals in real time, rather than later querying a database, either based on body-worn cameras or other surveillance by fixed or mobile devices.

The quantity of data and number of persons contained in facial recognition databases is immense, though the full scope is difficult to gauge. Law enforcement databases draw from a wide range of government sources, including drivers' licenses and mugshots gathered during previous police activity. A 2016 study found that nearly one in two US adults have had their photos searched by law enforcement via queries to state databases, including drivers' licenses.[3] Government Accountability Office (GAO) reports have shown that the FBI's FACE Services Unit can access in excess of 641 million images. Private sector databases, which are increasingly popular with police departments, draw from even more expansive sources. The Clearview app is reportedly based on a database of over three billion images "scraped" from public sources throughout the global Internet.[4]

What Is the Problem?

In recent years, the limitations of facial recognition technology, especially with regards to black, indigenous, and persons of color, have become part of mainstream conversation. The impacts of these limitations, especially when the technologies are used by organs of the state, can be significant. Advocates, academics, thoughtful observers, and even technology providers themselves, have pointed to hypothetical or actual instances in which these limitations can result in harm to individuals, up to and including infringement of rights. These harms can result from the design of the technology itself, databases and sources used, procedures and protocols concerning its use, or from real-world deployment scenarios which do not account for the limitations of the technology or possible incorrect use by police officers.

- **Transparency** - While a common practice in many jurisdictions, the full extent of how many agencies use facial recognition, and what data resources they have access to, is difficult to ascertain. The EFF and Georgetown Center on Privacy and Technology have described encountering multiple discrepancies, inconsistencies, and a refusal to disclose this information when researching the practices of state and federal authorities.[5] Without clarity on the scope of its use or clear agency policies guiding it, this lack of transparency undermines governance and accountability, as well as a systematic understanding of how widespread harms may be.

- **Algorithmic Bias and Inaccuracy** - Facial recognition systems exhibit different levels of accuracy based on conditions in the image, such as angle, lighting, resolution, and obscuring objects. Quality has improved markedly in these systems in recent years.[6] However, it is well documented that they tend to perform more poorly on faces with darker skin, as well as women, young children and the elderly. Much of this bias stems from training data used in the development of facial recognition systems, which commonly skews white and male, creating a systematic bias in the performance of algorithms. In 2018, Joy Buolamwini, founder of the Algorithmic Justice League and graduate of MIT's Media Lab, and Timnit Gebru of Microsoft Research, found that three major facial analysis technologies all performed most poorly when analyzing darker-skinned female subjects – demonstrating both skin-type and gender biases.[7] Further, a 2019 facial recognition study by NIST showed that among US-developed algorithms, there were high rates of false positives in one-to-one matching for Asians, African Americans and native groups.[8] This means that police queries may return false positives, misidentifications or false negatives, and that these errors are more likely to occur to those who are black, indigenous, and persons of color. Given that BIPOCs are more likely to come into contact with law enforcement, this means that they are more likely to face negative effects from being misidentified in encounters with the police.

- **Due process -** As facial recognition is still an emerging technology, its role in police investigations is not always clear, with some suggesting that in the absence of alternative evidence, investigators may rely too heavily on facial recognition databases and in some cases not disclose their use to defendants or their legal representatives.[9] Over-reliance on facial recognition can also influence human decisions. Recent research has shown that algorithmic face identity decisions influence subsequent human judgements about face similarity.[10] This could easily lead to confirmation bias among police officers, especially when acting solely on facial recognition for further action.

- **Invasion of privacy** - The broadening use of facial recognition can lead to individuals or groups feeling as if they are under constant surveillance, especially when it is unclear whether facial recognition technology is being used and for what purpose. Different data protection frameworks around the world may also require different levels of consent from individuals to the processing of their data (especially if facial biometric data is considered a special category of personal data requiring higher levels of protection.

- **Unbalancing the state/citizen relationship** - Facial recognition tools are increasingly being used by police because they can be highly useful. When other identifying information is limited, it provides law enforcement with the tools to rapidly identify some persons with a reasonable degree of certainty. However, when a tool provides this amount of power at such low cost to law enforcement – especially with unclear legal guardrails – the risk of abuse is high. It may unbalance the relationship between the state and individuals in public space and be used to chill dissent. In the context of BLM protests in New York City, for example, the NYPD utilized facial recognition to identify and track down a specific leader of the protest, besieging his private residence in a massive show of force to secure an arrest.[11]

What Do Stakeholders Think?

Technology Providers

On the topic of AI generally, major tech companies have been at the forefront of developing principles or codes of ethics to guide their use. Recently, these have been supplemented with additional voluntary restraints on how they use, develop, and sell facial recognition specifically – especially for law enforcement – as well as cautious calls for regulatory action. However, most of these voluntary restraints are designed to be temporary.

Amazon - "We're implementing a one-year moratorium on police use of Amazon's facial recognition technology... We've advocated that governments should put in place stronger regulations to govern the ethical use of facial recognition technology and, in recent days, Congress appears ready to take on this challenge. We hope this one-year moratorium might give Congress enough time to implement appropriate rules, and we stand ready to help if requested."[12]

IBM - Calling for "national dialogue" on whether or how facial recognition is used by law enforcement, IBM pledged to work with Congress to take action on general police reform, better skills training opportunities for communities of color, as well as "responsible technology policies" to increase transparency. Stating that vendors and users of AI have "shared responsibility" to ensure that AI is tested and audited for bias, "IBM no longer offers general purpose IBM facial recognition or analysis software. IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency."[13]

IBM's AI Fairness 360 is an open source toolkit that was launched in 2018 to help examine, report, and mitigate discrimination and bias in machine learning models and datasets.[14]

Google "share many of the widely-discussed concerns over the misuse of face recognition" and state "it's crucial that these technologies are developed and used responsibly." They argue that face-related technology must be fair and not reinforce or amplify bias, not be used in surveillance that violates internationally accepted norms, and should protect privacy, including transparency and control.[15]

Warning against "sweeping generalizations or simplistic solutions," they call for rigorous decision making processes when developing and deploying facial recognition, calling attention to five key dimensions: "(1) intended use; (2) notice, consent, and control; (3) data collection, storage, and sharing; (4) model performance and design; and (5) user interface. To complement this, Google also call for a "solutions-focused regulatory frameworks" that recognize nuances and encourage further innovation to improve privacy, fairness, and security.

Salesforce - As part of a series of commitments to improve its internal practices and external support for communities of color, Salesforce has dedicated a key pillar of its new taskforce to advocating for public policy reforms in areas such as policing, hate crimes, and criminal justice.[16]

Salesforce has also touted its decision not to develop and deploy facial recognition as a "conscious decision" that stems from "long held concerns about facial recognition technology, both around its accuracy and the harm it can cause, particularly to communities of color." They also cite its potential for use in political manipulation and discrimination in public places.[17]

Brad Smith has called for a "floor of responsibility" in order to support competiton without a "commercial race to the bottom"

Microsoft has long taken a strong public stance on facial recognition, lobbying for regulatory action at the state and federal level. Brad Smith has called for a "floor of responsibility," in order to support competition without a "commercial race to the bottom, with tech companies forced to choose between social responsibility and market success." To guide its own development market success." To guide its own development and use by customers, Microsoft has endorsed six key principles for managing facial recognition, namely: (1) fairness; (2) transparency; (3) accountability; (4) non-discrimination; (5) notice and consent; and (6) lawful surveillance.[18]

In response to recent concerns, Microsoft has pledged not to sell facial recognition technology to US police departments until there is a national law in place. At the state level, Microsoft strongly backed the recent Washington State measure addressing use of facial recognition by the public sector, which broadly tracked many of Microsoft's suggestions for a regulatory framework.[19]

Democratic Lawmakers

Democratic members of the House and Senate have taken a forward leaning stance on facial recognition issues, particularly as it pertains to its use by law enforcement. Democratic lawmakers have introduced and, in the case of the House of Representatives passed several measures, such as the George Floyd Justice in Policing Act. These measures generally place clear bars on federal usage of facial recognition, seek to restrict state and local uses, and place heightened standards on private sector development and deployment of facial recognition. Most measures (except the Notification Act) have been introduced and championed by Democrats.

Republican Lawmakers

Republicans have taken a more cautious approach. While calling for some measures, they have refrained from endorsing more stringent measures such as blanket bans. House Oversight Committee Ranking Member Jim Jordan has stated that use of facial recognition technology is an "urgent issue we must tackle is reining in the government's unchecked use of this technology when it impairs our freedoms and our liberties."[20] At minimum, he has called for a better understanding of how federal agencies use facial recognition and why.

Civil Society

Civil society and rights advocates encompass a broad range of groups, who adopt a range of approaches to facial recognition and law enforcement. Most organizations, especially those associated with the left, tend to advocate for either strict regulation and disclosure requirements, or outright bans on the use of facial recognition by law enforcement. However, even some on the right have suggested new curbs.

The ACLU and a coalition of civil society groups BanFacialRecognition.com led by Fight for the Future have called on Congress to ban the use of facial recognition by police departments and/or cut off any federal money for the purchase of such technology.[21] FFTF also benchmarks Congressional voting records on this topic,[22] and has called for a bar on use of facial recognition in schools and private sector deployments in public places without explicit, affirmative consent.[23] The Electronic Frontier Foundation has called attention to the pressing need for additional transparency on current use and meaningful safeguards to prevent misuse.[24] In addition to conducting a national survey of current law enforcement use of facial recognition with the Georgetown Center on Privacy and Technology, the EFF has launched a searchable database of police departments and the "Tech Tools They Use to Spy on Communities".[25]

Even organizations commonly considered to be on the right end of the political spectrum have raised concerns about the use of facial recognition technology. Commentary from American Enterprise Institute fellow Jim Harper has expressed concern that law enforcement use "will have to be very sharply tailored" in order to avoid infringing 4th Amendment standards.[26] The CATO Institute's Matthew Feeney has previously suggested that law enforcement use of facial recognition may need to be subject to a prohibition on real-time capability, restrictions on what databases can be searched, source code transparency and accuracy performance thresholds across multiple demographic groups.[27] By contrast, Nila Bala and Caleb Whatley of R Street have cautioned against an outright ban. While stating that "real safeguards" are needed, they argue that a ban would needlessly preclude the employment of a useful law enforcement tool. Nevertheless, they admit that a temporary moratorium may be appropriate as rules are developed, including a judicial approval process similar to warrants, minimum standards that preclude the use of facial recognition for minor offenses, and independent third-party testing.[28]

Advocates for BIPOCs

Organizations that advocate on behalf of the rights and advancement of Black Americans, Indigenous, and People of Color (BIPOC) share similar views to other civil society groups on this topic. Beyond bans, they also tend to focus strongly on the need for technology providers to have more inclusive development processes as a key element of mitigating bias and harms.

- Data for Black Lives has called on companies like Facebook to take steps to establish a Data Code of Ethics, hire more black data scientists and researchers, and create more transparency in their data practices.[29]

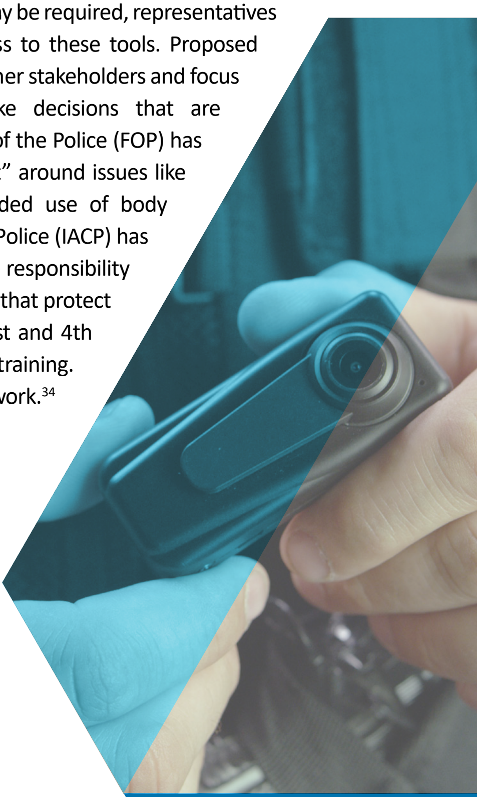
- Color of Change has led petitions to stop tech companies from providing technology to certain federal law enforcement agencies and prevent federal law enforcement from deploying these technologies in an effort to "stop the rise of Digital Jim Crow" and disproportionate negative effects on black residents and marginalized communities.[30]

- Congressional Black Caucus - Dating back to 2018, the CBC wrote directly to providers of facial recognition technology to express their concern regarding a "high propensity for misuse," call for "substantive dialogue," and encourage companies to hire more lawyers, engineers, and data scientists of color to rectify blindspots.[31]

- NAACP Legal Defense and Educational Fund has campaigned in support of immediate municipal-level bans on facial recognition and biometric surveillance, and improved public disclosures.[32]

Law Enforcement Organizations

While generally acknowledging that some reforms may be required, representatives of law enforcement are focused on retaining access to these tools. Proposed reforms are more limited than those suggested by other stakeholders and focus on empowering individual departments to make decisions that are appropriate for them. The National Fraternal Order of the Police (FOP) has expressed optimism that there is "broad agreement" around issues like "data collection, agency accreditation, and expanded use of body cameras."[33] The International Association of Chief of Police (IACP) has issued guiding principles on this topic, stating it is the responsibility of the user to develop "appropriate… usage policies" that protect constitutional rights of all persons, especially the 1st and 4th Amendments, as well as recommending mandatory training. It has released a Technology Policy Framework.[34]



What Are the Proposed Solutions?

Solving some of the challenges that facial recognition poses requires technical improvements to how these systems work. Companies and academics continually work to research, refine, and improve systems to mitigate bias. However, technical solutions cannot resolve all challenges with the technology. Policy solutions to contain harms from engrained bias in the near term as well as to curb abuses in its use are an indispensable component that technical solutions alone cannot resolve.

As a leading area of study and concern, facial recognition is one of the early focuses of regulatory responses to AI around the world. However, because of more immediate concerns, policy responses to use of facial recognition, particularly by law enforcement, are being discussed and adopted well in advance of wider AI regulation. These include a range of options:

- **Bans** - A simple, if drastic, solution is simply to ban the use of facial recognition technology by law enforcement, federal and/or state and local:

    - *All Uses of Facial Recognition* - The City of Portland recently became the most restrictive jurisdiction in the United States with regards to facial recognition. The City Council passed a complete ban on all public uses of facial recognition beginning immediately as well as a ban on all private sector uses within the city beginning 1 January 2021.[35]

    - *All Government Uses of Facial Recognition* - Several US states and localities have issued permanent or temporary bans on local government use, most notably the cities of San Francisco and Boston. The George Floyd Justice in Policing Bill[36] and other measures introduced primarily by Democrats in the US Congress would bar the use of facial recognition relating to federal law enforcement body cameras, or prohibit the use of federal funds to purchase facial recognition technology by police departments.

- *Certain Applications* - Particular concern has centered on the use of specific applications and companies supplying facial recognition technology, namely Clearview and its massive private database. In response, New Jersey and some others have not banned the use of facial recognition technology per se, but have issued a moratorium on police use of the Clearview facial recognition app.

- **Departmental Policies** - While some police departments may already have policies governing the use of artificial intelligence, this is not universal. Requiring that baseline policies be in place can create a mechanism for policy makers, civil society advocates, and other observers to hold police departments accountable. The IACP has called for each department to develop policies in accordance with the legal requirements of each jurisdiction.

- **Provider Transparency** - Providers of facial recognition technology could be required to publicly disclose a product's capabilities, limitations, certain performance metrics and any complaints or known defects. However, there are technical and standards-related challenges to developing such characteristics, including how to provide information that is meaningful to users while being sufficiently accurate and fit to purpose.

- **Deployer Transparency** - Without addressing difficult technical questions, transparency can also include procedural transparency, such as disclosure to citizens when they are in an area where police forces are using facial recognition technology or when it has been relied on in an investigation.

- **Proscribed Uses** - Certain uses of facial recognition technology may be so potentially injurious to fundamental rights that they should be specifically proscribed. Washington State, for example, recently passed a measure[37] forbidding the use of facial recognition techniques in three circumstances: to record the exercise of free speech and free assembly rights, when based on religion or political views, and when based on race or other protected class. Others have called for specific bans on the deployment of real-time facial recognition capabilities.

- **Warrant Requirements** - Use of facial recognition can be constrained by requiring law enforcement to obtain specific warrants in order to carry out monitoring based on established probable cause standards, barring exigent circumstances. This may prevent particularly injurious indiscriminate use. Similar standards were recently introduced by Washington State, with the backing of Microsoft.

- **Testing** - A robust ecosystem for third-party testing can help to shine a light on performance, driving competition to improve the capabilities of the technology and providing greater clarity to the buyer. This is especially important when facial recognition is used by the public sector. Mandated testing, or merely mandating the capability to be subjected to testing may be one route to create this ecosystem. For example, Washington State's new law requires that providers of facial recognition products to the public sector make available an open API to enable independent testing of their products' performance across different subgroups.

- **Industry Principles and Certification** - In addition to policy and legislative solutions, companies can develop facial recognition principles to foster consumer trust and help mitigate potential bias. WEF's 2020 Framework for Responsible Limits on Facial Recognition white paper lays out seven key areas – including privacy, risk assessment, proportional use, accountability, consent, accessibility, and adaptability – that should inform a company's "Principles for Action."[38] WEF moves beyond mere guidelines, by recommending an assessment and audit process through AFNOR Groupe to certify compliance. Microsoft, for example, published its own facial recognition principles in 2018, though the company has repeatedly called for governments to address facial recognition challenges as a necessary first step.[39] political views, and when based on race or other protected class. Others have called for specific bans on the deployment of real-time facial recognition capabilities.

Jurisdictions to Watch

Action addressing facial recognition, particularly public sector uses, is at the leading edge of AI regulation. Numerous jurisdictions in the United States and abroad have taken, or are contemplating, further actions. Some of the most notable to monitor include:

- **US Federal** - Congress has done little in the three months since major tech providers stepped back from facial recognition and is highly unlikely to do anything prior to the November 2020 election. Barring a revival of bipartisan talks on police reform, likely the only possible route available for facial recognition measures this year would be as attached to a major package such as another COVID relief bill or the National Defense Authorization Act. Whether one party has full control of Congress beginning in 2021 will be highly significant for whether legislators take action or remain at an impasse.

- **US State and Local** - Washington State recently become the first state to adopt a law to regulate facial recognition. Others are likely to follow in its wake, especially California, where the legislature is considering several bills which propose different approaches to the technology, ranging from a six year ban to affirmatively allowing its use by private businesses for security and safety without consent.

- **European Union** – The European Commission has prioritized regulatory action addressing AI. After the release of a white paper and consultation in the first half of 2020, they are advancing to developing legislative options for action, ranging from soft-law to targeted regulation of high risk applications.[40] While Brussels weighs the options, European law enforcement are also pushing to stitch together an EU network facial recognition database for law enforcement.[41]

Conclusions

Recent protests and the tech industry's response have made action on facial recognition, already a prior focus of policy makers in the US and elsewhere, a priority. While US Congressional action stalled and has been overtaken by the continued response to the pandemic and the US election season, this remains a space to watch. As the new Congress and administration execute an agenda, and especially as Amazon's one-year moratorium on police use draws to a close in mid-2021, pressure may rise for action. Despite a fragile consensus currently around temporary or permanent bans, the diversity of proposals and inherent technical challenges of some makes it difficult to envision likely outcomes.

Though the tech giants have sought to frame themselves as champions of privacy and consumer protection on facial recognition, the current status of facial recognition technology stands as a cautionary tale for how the development and deployment of technology may impact and be shaped by social and racial contexts. For new technologies to be equitable and sustainable, companies and policy makers need to carefully consider the full context in which it operates.

End Notes

[1] Greene, Jay. Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *The Washington Post*. Jun 11, 2020. https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.
[2] Letter to Jeff Bezos from American Civil Liberties Union (ACLU) *et al*. May 22, 2018. https://www.aclunc.org/docs/20180522_AR_Coalition_Letter.pdf.
[3] Garvie, Clare; Bedoya, Alvaro; Frankle, Jonathan. The Perpetual Lineup. Center on Privacy & Technology at Georgetown Law. 2016. https://www.perpetuallineup.org/.
[4] Hill, Kashmir. The Secretive Company That Might End Privacy as We Know It. *The New York Times*. Jan 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[5] See https://whohasyourface.org/about/#press and https://www.eff.org/deeplinks/2020/04/eff-testifies-law-enforcement-use-face-recognition-presidential-commission-law.
[6] Valentino-DeVries, Jennifer. How the Police Use Facial Recognition, and Where It Falls Short. *The New York Times*. Jan 12, 2020. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[7] Buolamwini, Joy; Gebru, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research.* 81:1–15, 2018. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[8] Grother, Patrick; Ngan, Mei; Hanaoka, Kayee. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. Dec 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[9] Valentino-DeVries, Jennifer. How the Police Use Facial Recognition, and Where It Falls Short. *The New York Times*. Jan 12, 2020. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[10] Howard, John J; Rabbit, Laura R; Sirotin, Yevgeniy B. Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making. *Plos One*. Aug 21, 2020. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0237855.
[11] Vincent, James. NYPD used facial recognition to track down Black Lives Matter activist. *The Verge*. Aug 18, 2020. https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.
[12] Announcement of one-year moratorium on police use of Recognition. Jun 10, 2020. https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition.
[13] CEO Arvind Krishna Letter to Congress on Racial Justice Reform. Jun 8, 2020. https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/.
[14] AI Fairness 360. IBM Research Trusted AI. https://aif360.mybluemix.net/resources.

[15] Google’s approach to facial recognition. https://ai.google/responsibilities/facial-recognition/.
[16] Beckwith, Ebony; Prophet, Tony. Taking Action for Racial Equality and Justice. Jun 10, 2020. https://www.salesforce.com/company/news-press/stories/2020/6/racial-equality-and-justice/.
[17] Goodman, Paula. Why We’ve Never Offered Facial Recognition. Jun 15, 2020. https://www.salesforce.com/company/news-press/stories/2020/6/salesforce-facial-recognition/.
[18] Smith, Brad. Facial recognition: It’s time for action. Dec 6, 2018. https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.
[19] Smith, Brad. Finally, progress on regulating facial recognition. Mar 31, 2020. https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/.
[20] Ranking Member Jim Jordan’s statement on facial recognition technology. Jan 15, 2020. https://republicans-oversight.house.gov/watch-ranking-member-jim-jordans-statement-on-facial-recognition-technology/.
[21] Legislation comes after Robert Williams shares story of being wrongfully arrested because of the flawed technology. Jun 25, 2020. https://www.aclu.org/press-releases/aclu-comment-bill-stopping-face-recognition-surveillance.
[22] Ban Facial Recognition activists launch congressional “scorecard” to name and shame lawmakers who have not endorsed legislation to stop face surveillance. Jul 22, 2020. https://www.fightforthefuture.org/news/2020-07-22-ban-facial-recognition-activists-launch/.
[23] Major new study calls for a ban on facial recognition in schools. Aug 10, 2020. https://www.fightforthefuture.org/news/2020-08-10-major-new-study-calls-for-a-ban-on-facial/.
[24] Lynch, Jennifer. EFF testifies today on law enforcement use of face recognition before Presidential Commission on Law Enforcement and the Administration of Justice. Apr 22, 2020. https://www.eff.org/deeplinks/2020/04/eff-testifies-law-enforcement-use-face-recognition-presidential-commission-law.
[25] EFF launches searchable database of police agencies and the tech tools they use to spy on communities. Jul 13, 2020. https://www.eff.org/press/releases/eff-launches-searchable-database-police-agencies-and-tech-tools-they-use-spy.
[26] Harper, Jim. Facial recognition’s reckoning, Fourth Amendment edition. Jan 23, 2020. https://www.aei.org/technology-and-innovation/facial-recognitions-reckoning-fourth-amendment-edition/].
[27] Feeney, Matthew. Should Police Facial Recognition be Banned? May 13, 2019. https://www.cato.org/blog/should-police-facial-recognition-be-banned.

[28] What are the proper limits on police use of facial recognition? Jun 20, 2019. https://www.rstreet.org/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/.
[29] COVID-19 Open Data by State. Data for Black Lives. https://d4bl.org/action.html.
[30] Ban of Facial Recognition Surveillance in Public Housing Necessary to Prevent Jim Crow Era Discrimination. https://colorofchange.org/press_release/color-of-change-ban-on-facial-recognition-surveillance-in-public-housing-necessary-to-prevent-jim-crow-era-discrimination/.
[31] CBC Expresses Privacy, Racial Bias Concerns about Facial Recognition Technology Marketed, Sold by Amazon. May 24, 2018. https://cbc.house.gov/news/documentsingle.aspx?DocumentID=898
[32] Reported NYPD Use of Powerful Surveillance Technology. Aug 2, 2019. https://www.naacpldf.org/press-release/ldf-responds-to-reported-nypd-use-of-powerful-surveillance-technology-on-photos-of-young-people/.
[33] National FOP President's Statement on Police Reform Legislative Efforts. Jun 25, 2020. https://fop.net/CmsDocument/Doc/pr_2020-0625.pdf.
[34] Guiding Principles for Law Enforcement's Use of Facial Recognition Technology. Jul 2019. https://www.theiacp.org/sites/default/files/2019-10/LE%20Facial%20Rec%20Guiding%20Principles%20Document%20July%202019.pdf.
[35] Peters, Jay. Portland passes strongest facial recognition ban in the US. *The Verge*. Sept 9, 2020. https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology.
[36] See Title III, Subtitle C, https://www.congress.gov/116/bills/hr7120/BILLS-116hr7120pcs.pdf.
[37] An act relating to the use of facial recognition services. http://lawfilesext.leg.wa.gov/biennium/2019-r0/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729.
[38] A Framework for Responsible Limits on Facial Recognition. World Economic Forum. Feb 2020. http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf.
[39] Smith, Brad. Facial recognition: It's time for action. Dec 6, 2018. https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.
[40] Artificial intelligence – Ethical and Legal Requirements. European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence.
[41] Campbell, Zach; Jones, Chris. Leaked reports show EU police are planning a pan-European network of facial recognition databases. *The Intercept*. Feb 21, 2020. https://theintercept.com/2020/02/21/eu-facial-recognition-database/.

We lead countries to fair tech

Access Partnership is the world's leading public policy firm dedicated to opening markets for technology. We shape national, regional and international policies to ensure a fair, long-lasting environment for technology that drives growth. Our teams in six offices across the globe uniquely mix policy and technical expertise to drive outcomes for clients operating at the intersection of technology, data and connectivity.

1730 Rhode Island Ave, NW
Suite 512
Washington, DC 20036
United States
Tel: (202) 503 1576

AccessAlerts
AccessPartnership

www.accesspartnership.com