Introduction

Amba Kak

Although the terminology varies,[1] we use the phrase biometric recognition technologies to describe systems that "fix"[2] official identities to bodily, physiological, or behavioral traits,[3] providing new ways for individuals to identify themselves, and also to be identified or tracked. While fingerprints have the longest history as a marker of identity and continue to be used in a number of applications across the world, other bodily markers like face, voice, and iris or retina are proliferating, with significant research exploring their potential large-scale application. Emerging areas of interest in this field include using behavioral biometrics like gait (i.e., how a person walks), keyboard keystroke patterns, and multimodal combinations of biometrics to identify and potentially make inferences about individuals.[4]

Beyond identifying people, these systems increasingly claim to be able to infer demographic characteristics, emotional states, and personality traits from bodily data. (This practice is sometimes referred to as "soft biometrics"[5] in technical literature.) In other words, there has been a change in questioning that historian Jane Caplan has summarized as a shift from "What person is that?" to "What *type* of person is that?"[6] Scholars have pointed to the fact that many of these systems that claim to detect interior characteristics from physical information are built

[1] The terms *biometric recognition*, *identification*, and *processing* are sometimes used interchangeably; other times, they are given more precise and distinct definitions. We use the umbrella terms biometric systems, biometric technologies, or biometric recognition (which has broad cachet in policy discourse) to cover the range of automated technologies that use biometric identifiers to identify, verify, or confirm a person's official identity. We also highlight open questions about whether systems that produce other kinds of inferences from bodily data (beyond official identity) should be included. This compendium does not analyze the regulation of DNA identifiers. While DNA is recognized as biometric information because of its ability to uniquely identify individuals, it is generally regulated under separate genetic privacy laws rather than biometric privacy laws, and its use in the criminal justice system has also been regulated under specific rules.

[2] See Aaron K. Martin and Edgar A. Whitley, "Fixing identity? Biometrics and the Tensions of Material Practices," *Media, Culture & Society* 35, no. 1 (2013): 52–60, https://doi.org/10.1177/0163443712464558.

[3] See Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: New York University Press, 2011), 19. Gates refers to systems of biometric recognition "as an index or recorded visual trace of a specific person."

[4] Riad I. Hammoud, Besma R. Abidi, Mongi A. Abidi, *Face Biometrics for Personal Identification: Multi-Sensory Multi-Modal Systems* (Berlin: Springer, 2007). See also sections on gait recognition and multimodal biometrics in *Global Biometric Authentication and Identification Market: Focus on Modality (Face, Eye, Fingerprint, Palm, and Vein), Motility, Application, and Technology Trends Analysis and Forecast: 2018–2023*, MarketResearch.com, March 2019, https://www.marketresearch.com/BIS-Research-v4011/Global-Biometric-Authentication-Identification-Focus-12342594/.

[5] *Soft biometrics* are defined as ancillary characteristics that provide some information, but not enough to identify a person. See Abdelgader Abdelwhab and Serestina Viriri, "A Survey on Soft Biometrics for Human Identification," in *Machine Learning and Biometrics*, ed. Jucheng Yang et al. (London: IntechOpen, 2018), https://doi.org/10.5772/intechopen.76021. See also U. Park and A. K. Jain, "Face Matching and Retrieval Using Soft Biometrics," *IEEE Transactions on Information Forensics and Security* 5, no. 3 (September 2010): 406–415, https://doi.org/10.1109/TIFS.2010.2049842. And see A. Dantcheva, "What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics," *IEEE Transactions on Information Forensics and Security* 11, no. 3 (March 2016): 441–467, https://doi.org/10.1109/TIFS.2015.2480381.

[6] Jane Caplan, "'This or That Particular Person': Protocols of Identification in Nineteenth-Century Europe," in *Documenting Individual Identity: The Development of State Practices in the Modern World*, ed. Jane Caplan and John Torpey (Princeton: Princeton University Press, 2001). Cf. Jake Goldenfein, Facial Recognition Is Only the Beginning, *Public Books*, January 27, 2020, https://www.publicbooks.org/facial-recognition-is-only-the-beginning/#fn-33473-10.

on debunked and racist scientific and cultural assumptions about who looks like what "type" of person,[7] and lead to demonstrated harms when applied in sensitive social domains like hiring or education.[8]

The rapid expansion of the biometrics industry coincides with advancing technical methods and features and decreasing costs of hardware and software. Camera- and video-analytics technologies being produced today are designed to have higher resolution, the ability to work from greater distances, and night-vision sensors that create the conditions for live facial recognition and real-time surveillance in public spaces.[9] Body-worn cameras that can attach to clothing or helmets have found a huge market among law enforcement agencies.[10] And advanced voice recorders that are able to pick up recordings from a greater distance are transforming voice recognition into a tool that could enable persistent remote surveillance.[11]

Meanwhile, the ubiquity of face photographs and voice recordings tagged with people's names on the internet has greatly decreased the financial and technical resources required to create the databases that underpin face and voice recognition systems. Clearview AI provides an example. The company was an inconspicuous start-up until it attracted global controversy in early 2020 for the three billion labeled face images (matched to names) it scraped from the web without consent. The company then used these photos to market surveillance tools to a range of private and public actors, claiming that its system could pull up identity and other intimate information about anyone whose image was in its database.[12] Recent reporting demonstrates that Clearview AI is not unique. In July 2020, the German digital rights blog Netzpolitik uncovered a Polish company called PimEyes that creates a similar "face search engine" with a database of nine hundred million images scraped from the web.[13] The magnitude of these companies' systems, along with their relative obscurity, demonstrates the way the market for biometric recognition systems consists of a number of nontransparent vendors that sell their systems globally without any oversight or scrutiny.[14]

[7] In June 2020, the civil society collective Coalition for Critical Technology called for publishers to stop all publication of computational research claiming to identify or predict "criminality" using biometric data. See Coalition for Critical Technology, "Abolish the #TechToPrisonPipeline," Medium, June 23, 2020, https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16. See also Lisa Feldman Barrett, Ralph Adochs, and Stacy Marsella, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements," *Psychological Science in the Public Interest* 20, no. 1 (July 2019): 1–68, https://doi.org/10.1177/1529100619832930; Zhimin Chen and David Whitney, "Tracking the Affective State of Unseen Persons," *Proceedings of the National Academy of Sciences*, February 5, 2019, https://www.pnas.org/content/pnas/early/2019/02/26/1812250116.full.pdf; Ruben van de Ven, "Choose How You Feel; You Have Seven Options," Institute of Network Cultures, January 25, 2017, https://networkcultures.org/longform/2017/01/25/choose-how-you-feel-you-have-seven-options/; and Lauren Rhue, "Racial Influence on Automated Perceptions of Emotions," *Race, AI, and Emotions*, November 9, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.

[8] See Jayne Williamson-Lee, "Amazon's A.I. Emotion-Recognition Software Confuses Expressions for Feelings," *OneZero*, Medium, October 28, 2019, https://onezero.medium.com/amazons-a-i-emotion-recognition-software-confuses-expressions-for-feelings-53e96007ca63; Fabio Fasoli and Peter Hegarty. "A Leader Doesn't Sound Lesbian!: The Impact of Sexual Orientation Vocal Cues on Heterosexual Persons' First Impression and Hiring Decision," *Psychology of Women Quarterly* 44, no. 2 (June 2020): 234–55, https://doi.org/10.1177/0361684319891168.

[9] See Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," ACLU, June 17, 2019, https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf. See also Kelly Gates, "Policing as Digital Platform," *Surveillance & Society* 17, no. 1/2 (2019), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12940.

[10] See Vivian Hung, Steven Babin, and Jacqueline Coberly, "A Market Survey on Body Worn Camera Technologies," National Institute of Justice, Johns Hopkins University Applied Physics Laboratory, November 2016, https://www.ncjrs.gov/pdffiles1/nij/grants/250381.pdf.

[11] Andreas Nautsch et al., "The GDPR & Speech Data: Reflections of Legal and Technology Communities, First Steps towards a Common Understanding," *Proc. Interspeech*, 2019, https://arxiv.org/abs/1907.03458.

[12] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[13] See Daniel Laufer and Sebastian Mainek, "A Polish Company Is Abolishing Our Anonymity," *NetzPolitik*, July 10, 2020, https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity/.

[14] See Dave Gershorm, "From RealPlayer to Toshiba, Tech Companies Cash in on the Facial Recognition Gold Rush," *OneZero*, Medium, June 2, 2020, https://onezero.medium.com/from-realplayer-to-toshiba-tech-companies-cash-in-on-the-facial-recognition-gold-rush-b40ab3e8f1e2.

A range of mostly proprietary algorithmic processes enable vendors to transform these databases into biometric recognition systems capable of identifying individuals at a large scale. Creating such a system requires a combination of human and computational labor, as well as a formidable technical, financial, and political infrastructure. Labeling and tagging biometric data in order to make it searchable and to prepare it to feed into machine learning systems requires significant, on-demand human labor power. There is no reliable way to create these systems without such labeled data. At present, much of this data labeling work, often contingent and underpaid, is outsourced to firms across the world, with a high concentration in countries in the Global South.[15] Using machine-learning techniques such as deep learning and readily available neural network architectures, these large datasets of images are used by firms to train and calibrate computer models that are designed and optimized to predict "matches" within a database, which in turn confirm or reveal identity.[16]

The frenzied growth of biometrics into a global multibillion-dollar industry has not happened organically.[17] Powerful state and private actors promote the belief that these technologies are effective, necessary, and beneficial. Their core claim is that a strong connection exists between bodily traits and identity, and that biometric identifiers can be uniquely attributed to a particular individual with a high degree of accuracy and continuity over time.[18] This claim is naturalized in biometric systems, as is the corollary belief that these digital technologies have lower chances of fraud compared to non-biometric and analog means of identification.

These claims of accuracy and efficiency are often taken as a given, and transposed onto broader societal and economic values like security, safety, and more efficient service delivery.[19] While fingerprints have the longest history as a marker of identity and continue to be used in a number of applications across the world,[20] other bodily markers like face, voice, and iris or retina are proliferating, with significant research exploring their potential large-scale application. Police agencies use data produced by facial recognition systems to identify suspects, make arrests, and confirm guilt or innocence through system matches.[21] It is also being used as a tool to do ID checks for those who lack identification documents,[22] to monitor large events or public spaces

[15] See Mary L. Gray and Siddharth Suri, *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass* (New York: Houghton Mifflin Harcourt, 2019); and Sarah T. Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (New Haven: Yale University Press, 2019).

[16] Neural network architectures like ResNet are widely available for training on individual datasets so developers can more quickly and efficiently build their own models. See Connor Shorten, "Introduction to ResNets," *Towards Data Science*, Medium, January 24, 2019, https://towardsdatascience.com/introduction-to-resnets-c0a830a288a4.

[17] Chris Burt, "Global Biometrics Revenues to Approach $43B by 2025: Market Research Briefs," BiometricUpdate.com, November 28, 2019, https://www.biometricupdate.com/201911/global-biometrics-revenues-to-approach-43b-by-2025-market-research-briefs.

[18] Sup. 3. Humans have always identified one another in part based on the way we look or sound. Kelly Gates explains how face recognition has proliferated in part because it digitized and automated an already existing documentary regime of face verification, where passport photos were routinely affixed to all manner of government identification documents.

[19] On the "securitization of identity," see generally Nikolas Rose, *Powers of Freedom: Reframing Political Thought* (Cambridge: Cambridge University Press, 1999).

[20] Simon A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Cambridge, MA: Harvard University Press, 2001).

[21] See Tom Wilson and Madhumita Murgia, "Uganda Confirms Use of Huawei Facial Recognition Cameras," *Financial Times*, August 20, 2019, https://www.ft.com/content/e20580de-c35f-11e9-a8e9-296ca66511c9; see also Robert Muggah and Pedro Augusto Pereira, "Brazil's Risky Bet on Tech to Fight Crime," *InSight Crime*, February 19, 2020, https://www.insightcrime.org/news/analysis/brazil-risky-tech-fight-crime/; Vidushi Marda, "View: From Protests to Chai, Facial Recognition Is Creeping Up on Us," *Economic Times*, January 7, 2020, https://carnegieindia.org/2020/01/07/view-from-protests-to-chai-facial-recognition-is-creeping-up-on-us-pub-80708; and Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," Georgetown Law, Center on Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/; Jonathan Hillman and Maesea McCalpin, "Watching Huawei's 'Safe Cities'," Center for Strategic & International Studies, November 4, 2019, https://www.csis.org/analysis/watching-huaweis-safe-cities.

[22] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

for known criminals, and to surveil protests.[23] Beyond face-based systems, a recent investigation revealed that dozens of prisons across the US were creating voice-print databases of inmates and applying voice recognition to their phone communication to detect when particular voice prints appear, track call recipients of interest, and even to identify external people who were contacting people in prison most often.[24] Meanwhile, amid an environment of heightened xenophobia and anti-immigrant political rhetoric, the use of biometrics is proliferating as a form of border control technology.[25] The rationale of security is by no means restricted to law and immigration enforcement. It has driven the use of these tools as access control technologies for workplaces, schools, and apartment complexes, where they automate identity verification and even evaluate behavior to determine entry permissions.[26]

In some ways, this growth and normalization of biometric recognition technology follows a similar trajectory to the rapid growth of closed-circuit television (CCTV) use through the 2000s, despite no clear evidence that it was effective in controlling crime. Security systems are often installed as a reaction to severe crimes, but without evidence that they would have prevented that crime in the first place. Indeed, research shows that the rapid proliferation of video surveillance followed from "crises, triggered by particular events such as, a child-kidnapping, a class-room murder, a terrorist outrage or rising concerns over crime."[27]

Today, governments across the world are the largest customer of the global biometrics industry, sustaining and shaping its growth. The development of tools for this wide range of government functions is typically outsourced to private firms that develop, market, and maintain these systems. A 2019 market-research report says that the "government segment is the highest revenue generating segment among all the applications of biometric authentication and identification."[28] Outside of security functions, governments are increasingly adopting biometric identifiers as a routine part of service delivery, with the active support of international development institutions and donor agencies. Biometric IDs are promoted as a means to prevent

[23] "As Global Protests Continue, Facial Recognition Technology Must Be Banned," Amnesty International, June 11, 2020, https://www.amnesty.org/en/latest/news/2020/06/usa-facial-recognition-ban/; Dave Gershgorn, "Facial Recognition Is Law Enforcement's Newest Weapon Against Protesters," *OneZero*, Medium, June 3, 2020, https://onezero.medium.com/facial-recognition-is-law-enforcements-newest-weapon-against-protestors-c7a9760e46eb; Blake Schmidt, "Hong Kong Police Have AI Facial Recognition Tech—Are They Using It against Protesters?," October 22, 2019, https://www.bloomberg.com/news/articles/2019-10-22/hong-kong-police-already-have-ai-tech-that-can-recognize-faces; Alexandra Ulmer and Zeba Siddiqui, "India's Use of Facial Recognition Tech during Protests Causes Stir," *Reuters*, February 17, 2020, https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ; Jameson Spivack, "Maryland's Face Recognition System Is One of the Most Invasive in the Nation" *Baltimore Sun*, March 9, 2020, https://www.baltimoresun.com/opinion/op-ed/bs-ed-op-0310-face-recognition-20200309-hg6jkfav2fdz3ccs55bvqjtnmu-story.html.

[24] George Joseph and Debbie Nathan, "Prisons across the US Are Quietly Building Databases of Incarcerated People's Voice Prints," *Intercept*, January 30, 2019, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/.

[25] Mark Latonero and Paula Kift, "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control," *Social Media + Society* 4, no. 1 (March 2018): 1–11, https://journals.sagepub.com/doi/full/10.1177/2056305118764432.

[26] Mark Maguire, "The Birth of Biometric Security," *Anthropology Today* 25, no. 2 (April 2009): 9–14, https://rai.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1467-8322.2009.00654.x; see generally BiometricUpdate.com, Access Control, https://www.biometricupdate.com/biometric-news/access-control-biometric-articles.

[27] Clive Norris, Mike McCahill, and David Wood, "The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Publicly Accessible Space," *Surveillance & Society* 2, no. 2/3 (2004), https://doi.org/10.24908/ss.v2i2/3.3369.

[28] The development of tools for government functions is typically outsourced to private firms that develop, market, and maintain these systems. See, e.g., "Global $52Bn Biometric Authentication & Identification Market, 2023: Focus on Modality, Motility, Application and Technology," *Business Wire*, April 10, 2019, https://www.businesswire.com/news/home/20190410005486/en/Global-52Bn-Biometric-Authentication-Identification-Market-2023.

service delivery fraud. Many of the ID systems are being rolled out in Global South countries—like in India, the Philippines, Kenya, and Brazil—and are not sector-specific, but are instead "general-purpose" IDs that construct a digital, biometric identity for each resident.[29]

Outside of government, biometric recognition systems have been normalized as part of everyday experiences, largely driven by the goal of preventing fraud. Biometric locks are now a staple feature of many smartphones and laptops, and biometric profiles of customers offer a way to uniquely identify individuals across their transactions online or at ATMs. Biometrics are also being promoted as a novel and promising consumer advertising technology,[30] where individuals can walk through cameras in a shopping space and be offered personalized advertising or be verified for loyalty programs seamlessly.[31]

The last few years mark a critical juncture, perhaps even a turning point, in the trajectory of continued biometric expansion. Civil-society advocates have challenged the foundational arguments made by companies and governments that produce and promote these technologies, highlighting the tangible harms caused by their use. Mounting research demonstrates that these systems perform poorly when used in real-life contexts,[32] even when the system meets narrow assessment standards that the industry relies on to back claims of accuracy.[33] Even systems that boast high accuracy rates have unevenly distributed errors. They perform less well on certain demographics than on others,[34] with particularly high failure rates for Black women, gender minorities, young and old people, members of the disabled community, and manual laborers.[35] Beyond accuracy, research and civil society are also challenging the dominant discourses

[29] See Frank Hersey, "2019: A Critical Year for Biometrics and Digital ID in the Global South," BiometricUpdate.com, December 23, 2019, https://www.biometricupdate.com/201912/2019-a-critical-year-for-biometrics-and-digital-id-in-the-global-south; and, for an analysis of several national biometric ID projects, see Alice Munyua and Udbhav Tiwari, "What Could an 'Open' ID System Look Like?: Recommendations and Guardrails for National Biometric ID Projects," *Open Policy & Advocacy*, January 20, 2020, https://blog.mozilla.org/netpolicy/2020/01/22/what-could-an-open-id-system-look-like-recommendations-and-guardrails-for-national-biometric-id-projects/.

[30] See Joseph Turow, *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power* (New Haven: Yale University Press, 2016). See also Robert Lee Angell and James R. Kraemer, "Using Biometric Data for a Customer to Improve Upsale Ad Cross-Sale of Items. US Patent US9031858B2," filed September 26, 2007, and issued May 12, 2015, https://patents.google.com/patent/US9031858B2/en.

[31] Justin Lee, "Touché Launches Biometrics-Based Loyalty and Payment Platform," BiometricUpdate.com, January 18, 2017, https://www.biometricupdate.com/201701/touche-launches-biometrics-based-loyalty-and-payment-platform; Esther Fung, "Shopping Centers Exploring Facial Recognition in Brave New World of Retail," *Wall Street Journal*, July 2, 2019, https://www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802.

[32] See, for example, "Face Off: The Lawless Growth of Facial Recognition in UK Policing," *Big Brother Watch*, May 2018, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. "The Metropolitan Police has the worst record, with less than 2% accuracy of its automated facial recognition 'matches' and over 98% of matches wrongly identifying innocent members of the public," the authors write. See also NIST, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. For error rates relating to biometric capture in India's Aadhaar project, see Anand Venkatanarayanan, "A Critical Examination of the State of Aadhaar 2018 Report by IDinsight," *Kaarana*, Medium, May 22, 2018, https://medium.com/karana/a-critical-examination-of-the-state-of-aadhaar-2018-report-by-idinsight-ef751e24d6c5.

[33] Inioluwa Deborah Raji and Genevieve Fried, "About Face: A Survey of Facial Recognition Evaluation," Meta-Evaluation workshop at AAAI Conference on Artificial Intelligence, 2020.

[34] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018):1–15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; KS Krishnapriya et al., "Characterizing the Variability in Face Recognition Accuracy Relative to Race," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (2019), https://arxiv.org/abs/1904.07325; Cynthia M. Cook et al., "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science* 1, no. 1 (Jan. 2019): 32–41, https://ieeexplore.ieee.org/document/8636231; Inioluwa Deborah Raji and Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *Proceedings of the Conf. on Artificial Intelligence, Ethics, and Society* (2019), https://www.aies-conference.com/2019/wp-content/uploads/2019/01/AIES-19_paper_223.pdf; Morgan Klaus Scheuerman, Jacob M. Paul, and Jed R. Brubaker, "How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services," *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019): 1–33, https://doi.org/10.1145/3359246.

[35] Ursula Rao, "Biometric Bodies, or How to Make Electronic Fingerprinting Work in India," *Body & Society* 24, no. 3 (September 2018): 68–94, https://doi.org/10.1177/1357034X18780983.

of security, safety, and efficiency that have driven marketing and demand for these systems. Advocates are increasingly asking for whom such systems provide safety and security. The claim that biometric surveillance "makes communities safer" is heavily marketed but loosely backed. Companies and governments make access to details on these systems and their use difficult to obtain, but even so, there is strong evidence that these systems are being deployed in ways that harm historically marginalized people and communities. For example, in the US, there have been multiple cases where facial recognition has resulted in misidentification of suspects, including cases where facial recognition is used as primary evidence to determine guilt.[36] This harm is compounded by the systematic denial of basic due process rights during trial, in which defendants are denied access to information about whether and how these systems were used.[37] Even outside of law enforcement, there is no transparency at all when it comes to privately created "watch list" databases, which are likely being shared and institutionalized through their use at large-scale events, retail stores, and housing complexes. At a recent Taylor Swift concert, all attendees were subject to facial recognition without their knowledge or consent, creating public debate around the lack of safeguards people would have recourse to if they were blacklisted unfairly by these systems.[38]

As new applications of these technologies are created, so are new forms of pushback. Real-time monitoring of protests with facial recognition (e.g., in Hong Kong,[39] Delhi,[40] Detroit,[41] and Baltimore[42]) has been met by fierce community opposition. This type of pervasive real-time surveillance can potentially produce chilling effects on the democratic exercise of rights to free speech and movement in public life. Organized tenants groups have contested the use of facial recognition and other property technologies ("PropTech") to control access to residential buildings, arguing that they provide landlords with greater unaccountable control, and the ability to harass and surveil tenants.[43] Meanwhile, coalitions between digital-rights organizations and social welfare and accountability activists have challenged biometric ID schemes for social service

[36] Kashmir Hill, "Wrongfully Accused by an Algorithm," *New York Times*, June 24, 2020 https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Rashida Richardson, Jason M. Schultz, and Vincent M. Southerland, "Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems," AI Now Institute, September 2019, https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf; Bob Van Voris, "Apple Face-Recognition Blamed by N.Y. Teen for False Arrest," *Bloomberg*, April 22, 2019, https://www.bloomberg.com/news/articles/2019-04-22/apple-face-recognition-blamed-by-new-york-teen-for-false-arrest; Jeremy C. Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect," *Boston Globe*, April 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

[37] For an analysis of criminal due process in the context of facial recognition, see Emma Lux, "Facing the Future: Facial Recognition Technology Under the Confrontation Clause," *American Criminal Law Review* 57, no. 0 (Winter 2020), https://www.law.georgetown.edu/american-criminal-law-review/sample-page/facing-the-future-facial-recognition-technology-under-the-confrontation-clause/.

[38] See Jay Stanley, "The Problem with Using Face Recognition on Fans at a Taylor Swift Concert," ACLU, December 14, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/problem-using-face-recognition-fans-taylor-swift; and Parmy Olson, "Facial Recognition's Next Big Play: The Sports Stadium," *Wall Street Journal*, August 1, 2020, https://www.wsj.com/articles/facial-recognitions-next-big-play-the-sports-stadium-11596290400.

[39] Blake Schmidt, "Hong Kong Police Already Have AI Tech that Can Recognize Faces," *Bloomberg*, October 22, 2019, https://www.bloomberg.com/news/articles/2019-10-22/hong-kong-police-already-have-ai-tech-that-can-recognize-faces.

[40] Alexandra Ulmer and Zeba Siddiqui, "India's Use of Facial Recognition Tech During Protests Causes Stir," Reuters, February 17, 2020, https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ.

[41] "Protesters Demand to Discontinue Facial Recognition Technology," CBS Detroit, June 16, 2020, https://www.newsbreak.com/michigan/detroit/news/0PLepn7b/protesters-demand-to-discontinue-facial-recognition-technology.

[42] Spivack, "Maryland's Face Recognition System Is One of the Most Invasive in the Nation."

[43] Tranae Moran, Fabian Rogers, and Mona Patel, "Tenants Against Facial Recognition," AI Now 2019 Symposium, October 2, 2019, https://ainowinstitute.org/symposia/videos/tenants-against-facial-recognition.html; Erin McElroy, Meredith Whittaker, and Genevieve Fried, "COVID-19 Crisis Capitalism Comes to Real Estate," *Boston Review*, May 7, 2020, http://bostonreview.net/class-inequality-science-nature/erin-mcelroy-meredith-whittaker-genevieve-fried-covid-19-crisis.

delivery on the basis of their impacts on privacy as well as the denial of basic entitlements due to technical or operational failures in these systems.[44] Advocacy campaigns continue to question the use of facial recognition at airports, as well as the reuse of driver's licenses and other civilian biometric databases for immigration enforcement and private investigation purposes.[45]

While public advocacy is increasing in many parts of the world, and each campaign has its unique characteristics related to local political and economic contexts, what unites the current wave of pushback is the insistence that these technologies *are not inevitable*. Questioning technological inevitability has become a popular refrain, and reminds those acquiring, promoting, and regulating these systems that the future course of these technologies must and will be subject to greater democratic control.

Calls for regulation include demands to introduce new laws (e.g., like data-protection frameworks); to reform and update existing laws (e.g., laws that currently only regulate fingerprints and DNA use in the criminal process); to pause these systems; or to outright ban their use. In Kenya and India, there have been demands to pass data-protection laws amid the rollout of large-scale biometric ID projects without such laws in place.[46] Parliamentarians and government officials in the UK[47] and a government-appointed advisory group in Scotland have acknowledged the need for a broad regulatory framework for biometric use, alongside the need to update existing laws that only apply to fingerprint and DNA biometrics.[48] The clearest pushback on the idea that these technologies are inevitable has come in the form of advocacy championing complete bans or moratoria on the use of these systems, irrespective of context.[49] Similarly, while

[44] See Jamaican Supreme Court Decision, Julian Robinson v. Attorney General of Jamaica [2019] JMFC Full 04, https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf; Indian Supreme Court decision, K. S. Puttaswamy v. Union of India, Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, https://indiankanoon.org/doc/127517806/; see also #WhyID, "An Open Letter to the Leaders of International Development Banks, the United Nations, International Aid Organisations, Funding Agencies, and National Governments," Access Now, https://www.accessnow.org/whyid-letter/.

[45] See Project South, "Georgia Department of Driver's Services Colludes with Immigration and Customs Enforcement and Law Enforcement Agencies," 2020, https://projectsouth.org/wp-content/uploads/2020/03/GA-DDS-ICE-Fact-Sheet-.pdf; Joseph Cox, "DMVs Are Selling Your Data to Private Investigators," *Vice*, September 6, 2019, https://www.vice.com/en_us/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars; Drew Harwell and Erin Cox, "ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers," *Washington Post*, February 26, 2020 https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/; Sushovan Sircar, "Selling Vehicle Owners' Data as 'Public Good', Govt Earns Rs 65 Cr," *Quint*, July 10, 2015, https://www.thequint.com/news/india/ministry-of-transport-and-highways-rs-65-crore-driving-license-vehicle-registration-bulk-data-sale; "Opposition to Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns," ACLU, n.d., https://www.aclu.org/other/opposition-face-recognition-software-airports-due-ineffectiveness-and-privacy-concerns.

[46] See, e.g., Christine Mungai, "Kenya's Huduma: Data Commodification and Government Tyranny," *Al Jazeera*, August 6, 2019, https://www.aljazeera.com/indepth/opinion/kenya-huduma-data-commodification-government-tyranny-190806134307370.html; Vrinda Bhandari, "Why Amend the Aadhaar Act without First Passing a Data Protection Bill?," *The Wire*, January 4, 2019, https://thewire.in/law/aadhaar-act-amendment-data-protection.

[47] "The Future of Biometrics," *UK Parliament Post*, February 6, 2019, https://www.parliament.uk/documents/post/Future%20of%20Biometrics_notes%20from%20briefing%20event_final.pdf; Claire Cohen, "Public Expect Police to Be Using Facial Recognition Technology after Seeing It in Spy Thrillers Like James Bond, Says Cressida Dick," *Telegraph*, June 3, 2019, https://www.telegraph.co.uk/news/2019/06/03/public-expect-police-using-facial-recognition-technology-seeing/.

[48] Scottish Government, "Independent Advisory Group on the Use of Biometric Data in Scotland," March 2018, https://www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2018/03/report-independent-advisory-group-use-biometric-data-scotland/documents/00533063-pdf/00533063-pdf/govscot%3Adocument/00533063.pdf.

[49] See generally Melina Sebastian, "Normalizing Resistance: Saying No to Facial Recognition Technology," *Feminist Media Studies* 20, no. 4 (May 2020): 594–597; Ban Facial Recognition, https://www.banfacialrecognition.com/; Big Brother Watch, Stop Facial Recognition, n.d., https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/; Urvashi Aneja and Angelina Chamauh, "We Need to Ban Facial Recognition Altogether, Not Just Regulate Its Use," Tandem Research India, January 19, 2020, https://tandemresearch.org/publications/we-need-to-ban-facial-recognition-altogether-not-just-regulate-its-use.

a recent Indian Supreme Court decision eventually upheld the constitutionality of the country's biometric ID project, a dissenting opinion from one of the judges also made clear that it's not too late to turn back, ordering that "all such data be destroyed."[50]

Advocacy and the threat of regulation have spurred companies to act proactively to mitigate, and potentially undercut or postpone, demands for prohibition or strict regulation. Microsoft and Amazon have released calculated public statements in support of facial recognition regulation.[51] More recently, IBM, Microsoft, Amazon, and others committed to pause their use of these technologies, citing disproportionate harms to people of color amid widespread antiracist Black Lives Matter mobilization in the US and around the globe.[52] Activists responded by reminding legislators that these voluntary gestures were not nearly enough: "Facial recognition, like American policing as we know it, must go."[53]

Amid heightened public scrutiny, interest in regulating biometric technologies has grown significantly. The degree of openness to legislating technology varies, and for some countries regulation is not a realistic or appropriate intervention at all. Yet in many parts of the world, the next few years do seem poised to produce wide ranging regulation and with that, offer the possibility to alter the future course of biometric technologies. This compendium responds to this environment of possibility, compiling detailed case studies of existing attempts to regulate biometric systems that post emergent and open questions for the future.

[50] Justice Chandrachur (dissenting opinion) in K. S. Puttaswamy v. Union of India , Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, https://indiankanoon.org/doc/127517806/; see also Ashok Kini, "Jamaican SC Quotes Justice Chandrachud's Dissent to Strike Down Aadhaar-Like Programme," *The Wire*, April 13, 2019, https://thewire.in/law/jamaica-supreme-court-aadhaar-justice-chandrachud.

[51] Often these companies publicly champion the need for some "regulation" but simultaneously lobby against moratoria and bans.

[52] Kate Kaye, "IBM, Microsoft, and Amazon's Face Recognition Bans Don't Go Far Enough," *Fast Company*, June 13, 2020, https://www.fastcompany.com/90516450/ibm-microsoft-and-amazons-face-recognition-bans-dont-go-far-enough.

[53] Malkia Devich-Cyril, "Defund Facial Recognigion," *Atlantic*, July 5, 2020, https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/.

This collection of eight essays from diverse contributors covers widely divergent contexts:

Australian Identity-Matching Services Bill: *Jake Goldenfein (Melbourne Law School)* and *Monique Mann (Deakin University)* track the institutional and political maneuvers that resulted in Australia's ambitious centralized facial recognition program ("The Capability"). They draw lessons from what they term the "futility of regulatory oversight."

The Economy (and Regulatory Practice) That Biometrics Inspires: A Study of the Aadhaar Project: *Nayantara Ranganathan (lawyer and independent researcher, India)* explains how law and policy around India's Biometric ID ("Aadhaar") project eventually served to construct biometric data as a resource for value extraction by private companies. She explores how regulation was influenced by the logics and cultures of the project it sought to regulate.

A First Attempt at Regulating Biometric Data in the European Union: *Els Kindt (KU Leuven)* provides a detailed account of the European Union's General Data Protection Regulation (GDPR) approach to regulating biometric data. As many countries are set to implement similarly worded national laws, she warns of potential loopholes and highlights key areas for reform.

Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases: *Ben Hayes (AWO Agency, Consultant legal advisor to the International Committee of the Red Cross [ICRC])* and *Massimo Marelli (Head of the ICRC Data Protection Office)* explain ICRC's decision-making process as they formulated the institution's first biometrics policy in the context of humanitarian assistance, with a focus on minimizing the creation of databases and risks to vulnerable populations.

Policing Uses of Live Facial Recognition in the United Kingdom: *Peter Fussey (University of Essex)* and *Daragh Murray (University of Essex)*, lead authors of the independent empirical review of the London Metropolitan Police's trial of Live Facial Recognition (LFR), explain how existing legal norms and regulatory tools fell short, with broader lessons for the regulation of LFR in the UK and elsewhere.

A Taxonomy of Legislative Approaches to Face Recognition in the United States: *Jameson Spivack and Clare Garvie (Georgetown Center on Privacy and Technology)* write about the dozens of bans and moratoria legislation on police use of facial recognition in the US, providing a detailed taxonomy that goes beyond these broad categories, and lessons learned from their implementation.

BIPA: The Most Important Biometric Privacy Law in the US? *Woodrow Hartzog (Northeastern University)* explores the promise and pitfalls of the State of Illinois' Biometric Information Privacy Act (BIPA) and, more broadly, of the private right of action model. He questions the inevitable limits of a law that is centered on notice and consent.

Bottom-Up Biometric Regulation: A Community's Response to Using Face Surveillance in Schools: *Stefanie Coyle (NYCLU)* and *Rashida Richardson (Rutgers University, AI Now Institute, NYU)* examine the controversial move by a school district in Lockport, New York, to implement a facial and object recognition system. They highlight the community-driven response that incited a national debate and led to statewide legislation regulating the use of biometric technologies in schools.