

The logo for AINOW, featuring the word in a stylized, outlined font.

REGULATING² BIOMETRICS

Global Approaches and Urgent Questions³

REGULATING BIOMETRICS¹

Global Approaches and Urgent Questions

Edited by Amba Kak²

September 2020³

Cite as: Amba Kak, ed., “Regulating Biometrics: Global Approaches and Urgent Questions” AI Now Institute, September 1 2020, <https://ainowinstitute.org/regulatingbiometrics.html>.⁴

ACKNOWLEDGMENTS⁵

I would like to acknowledge and thank **Luke Strathmann** for his steadfast editorial support, without which this compendium would not have come together. Thanks also to **Caren Litherland** for her meticulous copyediting. I’m immensely grateful to the authors of the chapters in this compendium for their seamless collaboration, despite an unexpectedly challenging year in the midst of a pandemic. I’m equally grateful, as always, to my colleagues **Meredith Whittaker**, **Alejandro Calcaño**, **Theodora Dryer**, **Sarah Myers West**, **Varoon Mathur**, and **Inioluwa Deborah Raji** for their detailed feedback and edits; and to **Jason Schultz** and **Kate Crawford** for their guidance on an earlier draft. A special thank you to **Carly Kind** (Ada Lovelace Institute), **Ella Jakubowska** (EDRI), and **Vidushi Marda** (Article 19) for their generous feedback on the introductory chapter.⁶

ARTWORK⁷

The images used on the cover and throughout this compendium are by **Heather Dewey-Hagborg**,⁸ Visiting Assistant Professor of Interactive Media at NYU Abu Dhabi and Artist Fellow at AI Now.

In *How Do You See Me?* Dewey-Hagborg developed custom software to produce a series of images that are detected as “faces” or are recognized as her. Starting from primitive curves and gradients, images evolve to more strongly elicit the algorithmic detection and recognition response.⁹

We see the face reduced to a white circle, laying bare the racial assumptions that underpin facial detection technologies.¹⁰

And we see abstract shapes and patterns, images that seemingly bear no resemblance to faces, emerge as neighboring facial vectors to the artist’s own.¹¹

The outcome of these experiments is a series of images that give us a window into how we are seen by the opaque technologies of artificial intelligence and facial recognition.¹²

Learn more about the project at <https://deweyhagborg.com/projects/how-do-you-see-me>.¹³



This work is licensed under a [Creative Commons Attribution-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nd/4.0/)

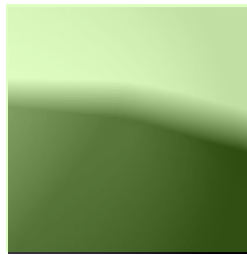
NOTE FROM THE EDITOR¹

Amid heightened public scrutiny, interest in regulating biometric technologies has grown across the globe. Public advocacy has driven this scrutiny across globally dispersed and distinctive local political contexts. Common across these diverse movements is a growing sense that these technologies are no longer inevitable, accompanied by questions as to whether they are necessary at all. Advocates continue to remind developers, profiteers, and those using and regulating these biometric systems that the future course of these technologies must—and will—be subject to greater democratic control. The next few years are poised to produce wide-ranging legal regulation in many parts of the world that could alter the future course of these technologies. **Addressing this moment of possibility, this compendium presents eight case studies from academics, advocates, and policy experts offering a variety of perspectives and national contexts. These expert contributors illuminate existing attempts to regulate biometric systems, and reflect on the promise, and the limits, of the law.**

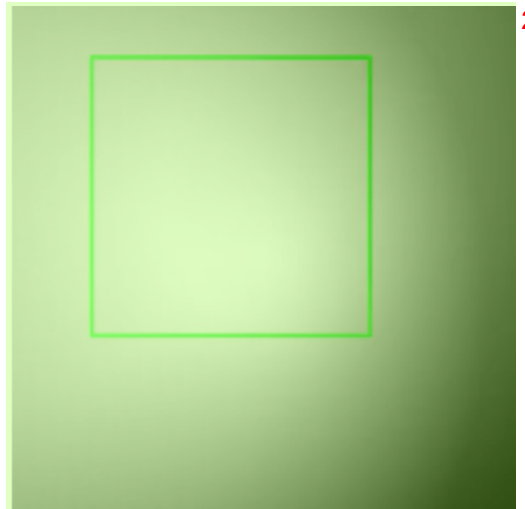
The compendium begins with an introduction and a summary chapter that identifies key themes from existing legal approaches, and poses open questions for the future. These questions highlight the critical research needed to inform ongoing national policy and advocacy efforts to regulate biometric recognition technologies.

CONTENTS¹

Chapter 0.		3
Introduction		6
<i>Amba Kak</i>		
Chapter 1.		4
The State of Play and Open Questions for the Future	16	
Timeline of Legal Developments	42	
<i>Amba Kak</i>		
Chapter 2.		5
Australian Identity-Matching Services Bill	44	
<i>Jake Goldenfein and Monique Mann</i>		
Chapter 3.		6
The Economy (and Regulatory Practice) That Biometrics Inspires: A Study of the Aadhaar Project	52	
<i>Nayantara Ranganathan</i>		
Chapter 4.		7
A First Attempt at Regulating Biometric Data in the European Union	62	
<i>Els Kindt</i>		
Chapter 5.		8
Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases	70	
<i>Ben Hayes and Massimo Marelli</i>		
Chapter 6.		9
Policing Uses of Live Facial Recognition in the United Kingdom	78	
<i>Peter Fussey and Daragh Murray</i>		
Chapter 7. A Taxonomy of Legislative Approaches to Face Recognition in the United States	86	10
<i>Jameson Spivack and Clare Garvie</i>		
Chapter 8.		11
BIPA: The Most Important Biometric Privacy Law in the US?	96	
<i>Woodrow Hartzog</i>		
Chapter 9.		12
Bottom-Up Biometric Regulation: A Community's Response to Using Face Surveillance in Schools	104	
<i>Stefanie Coyle and Rashida Richardson</i>		



1



2



3

Introduction¹

Amba Kak²

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.¹⁵ 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 Gershgorin, “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 1 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 2 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 3 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 Muniya 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 Baltimore⁴²) 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-mistakenly-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-recognition-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 UK⁴⁷ 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/43kxq/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-core-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 Chamaiah, "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 1

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 2

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. 3

50 Justice Chandrachud (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 Recognition," *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: ¹

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." ²

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. ³

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. ⁴

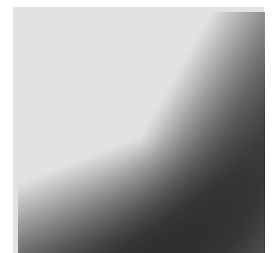
Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases: *Ben Hayes (AWO Agency, Consultant legal advisor to the International Committee of the Red Cross [ICRC]) and Massimo Marelli (Head of the ICRC Data Protection Office)* explain ICRC's decision-making 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. ⁵

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. ⁶

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. ⁷

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. ⁸

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. ⁹ ¹⁰



The State of Play and Open Questions for the Future¹

Amba Kak²

This chapter synthesizes broad trends and open questions for the regulation of biometric systems. We draw insights primarily from the essays in this compendium to surface lessons from existing legal approaches across multiple countries and contexts. Beyond analysis of the current state of play, we pose open questions about where regulation needs revision, or reimagination. We explore the rapidly evolving policy conversation around new kinds of regulatory interventions but also, crucially, the limits of the law in capturing or resolving concerns about these technologies.³

Regulation of biometric systems has largely been through data-protection laws. Biometric data is typically designated as an especially sensitive category of personal data and is regulated through a series of restrictions on the collection, retention, and disclosure of such data.¹ The 2016 European Union's General Data Protection law (GDPR) is emblematic of this approach, and there are currently over 140 countries with national data-protection laws that cover private- and public-sector use of data.² The United States lacks a comprehensive federal data privacy regulation similar to the GDPR, but state laws like the 2018 Illinois Biometric Information Privacy Act (BIPA)⁴

¹ 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 Graham Greenleaf and Bertil Cottier, "2020 Ends a Decade of 62 New Data Privacy Laws," *Privacy Laws & Business International Report* 163, no. 24-26 (January 29, 2020), <https://ssrn.com/abstract=3572611>. (According to this research, the count was at 142 at the end of 2019.)

follow a similar data-protection approach to regulating biometric data.³ Key elements of this approach are also included in laws that establish and govern biometric ID systems like India's 2016 Aadhaar Act,⁴ Australia's 2019 Identity Services Matching Bill,⁵ and Kenya's 2019 Huduma Namba bill.⁶ **Section 1** ("The Data-Protection Lens") examines these approaches to regulating biometrics, highlighting key concerns that have become apparent through their implementation.

While data-protection laws have made fundamental shifts in the way companies and government approach the collection, retention, and use of personal data, there are clear limitations on their ability to address the full spectrum of potential harms produced by new forms of data-driven technology, like biometric identification and analysis. Their focus on individual (rather than group) conceptions of harm fails to meaningfully address questions of discrimination and algorithmic profiling.⁷ The focus on data as the object of regulation has also sometimes obscured the broader challenges to social and institutional practices that these systems and platforms exert on society, in which imperfect but established methods of accountability, contestation, and democratic decision-making are undercut by the introduction of opaque automated technology.⁸ In contrast, there has been a flurry of legislation, mostly in the United States, that bans the use of these systems in particular sectors, across certain uses, or for lengths of time until there is a more participatory and deliberative process of decision-making in place. Sector-specific rules have also emerged, like those that address the harms of biometric systems in criminal justice or employment or education domains. **Sections 2 and 3 of this chapter** track these emergent concerns and legal approaches.

3 Illinois Biometric Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15. Texas and Washington have passed similar biometric privacy laws (see Tex. Bus. & Com. Code §503.001; Wash. Rev. Code Ann. §19.375.020). Proposals like the Florida Biometric Privacy Act, Bill S.1385 in Massachusetts, and New York Biometric Privacy Act NY SB 1203 in New York are also explicitly modeled after BIPA. For other examples of a data privacy approach to biometric data, see California Consumer Privacy Act of 2018 (CCPA) [1798.100 - 1798.199]; N.Y. 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act; N.Y. Lab. Law §201 (prohibiting fingerprinting as a condition of employment); Arkansas Code §4-110-103(7). On August 4 2020, as this compendium was going into print, the National Biometric Privacy Act was introduced by Senators Bernie Sanders and Jeff Merkley along similar lines to BIPA. See The National Law Review, "National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley and Bernie Sanders", The National Law Review, August 5, 2020 <https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie>.

4 Ministry of Law and Justice (Legislative Department), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Pub. L. No. 18 of 2016, https://uidai.gov.in/images/the-aadhaar_act_2016.pdf.

5 Parliament of Australia, "Identity-Matching Services Bill 2019 (Cth)," https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6387.

6 The Huduma Bill, 2019, <https://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf>.

7 See generally Martin Tisné, "The Data Delusion: Protecting Individual Data Isn't Enough When the Harm Is Collective," Stanford Cyber Policy Center, n.d., https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf; Linnet Taylor, Luciano Floridi, and Bart van der Sloot, eds., *Group Privacy: New Challenges of Data Technologies* (Cham: Springer, 2016), <https://www.springer.com/gp/book/9783319466064>; Brent Mittelstadt, "From Individual to Group Privacy in Big Data Analytics," *Philosophy & Technology* 30, no. 4 (February 2017): 475–494, <https://link.springer.com/article/10.1007/s13347-017-0253-7>.

8 See generally Amba Kak and Rashida Richardson, "Artificial Intelligence Policies Must Focus on Impact and Accountability," CIGI Online, May 1, 2020, <https://www.cigionline.org/articles/artificial-intelligence-policies-must-focus-impact-and-accountability>.

The following is a summary of the questions that this compendium raises, pointing to research, regulation, and community engagement that will be needed to inform ongoing national policy and advocacy efforts:

1. The Data-Protection Lens ²

- How should regulation define “biometric data”?
- Why have data protection laws had limited effectiveness in curbing the expansion of biometric surveillance infrastructure by government?
- Is meaningful notice and consent possible in the context of biometric systems? What are the limitations of a consent-based approach and what supplements or alternatives might be required?

2. Beyond Privacy: Accuracy, Discrimination, Human Review, and Due Process ⁴

- How should regulatory frameworks address concerns about accuracy and non-discrimination in biometric systems?
- To what extent should regulation rely on standards of performance and accuracy set by technical standards-setting bodies?
- Does requiring “meaningful human review” of biometric recognition systems ensure oversight and accountability?
- Should regulatory frameworks create a risk-based classification between “identification” and “verification” uses of biometric recognition?
 - What are the potential risks of a permissive regulatory approach to verification?
- What kinds of due process safeguards are required for law enforcement use of biometric recognition?
 - Should law enforcement have access to these systems to begin with?
- Are systems that process bodily data for purposes beyond establishing individual identity, like making inferences around emotional state, personality traits, or demographic characteristics covered under existing biometric regulation?
 - Should such systems be permitted at all, given their contested scientific foundations and mounting evidence of harm?

3. Emerging Regulatory Tools and Enforcement Mechanisms ⁶

- What different types of “bans” and moratoria have been passed in the US over the past few years?
 - How can moratoria conditions be strengthened to ensure that eventual legislative or deliberative processes are robust?
- How will bans and moratoria on government use impact the private development and production of biometric systems?
- What regulatory tools can be used to create public transparency around the development, purchase, and use of biometric recognition tools?
- What role can community-led advocacy play in shaping the priorities and impact of regulation?

SECTION 1. THE DATA-PROTECTION LENS¹

How should regulation define “biometric data”?²

*Under the dominant data-protection approach to regulating biometric systems, meeting the definition of “biometric data” has been the threshold condition for legal protections to apply. Recent regulatory attempts move away from this with “systems” rather than data as the object of regulation.*³

*In laws that establish and regulate biometric ID systems, the definition of biometric data has typically been left open-ended to allow governments to add or change the types of biometrics collected under these projects.*⁴

In defining biometric data and systems, the law not only reflects but also entrenches certain perceptions about the stability and accuracy of biometrics as an identification technology. For example, the GDPR states that biometric data is bodily, physiological, and behavioral data that “allow or confirm the unique identification of that natural person,”⁹ while the Illinois BIPA provides an exhaustive list of identifiers that count as biometric data and requires that they are “used to identify an individual.”¹⁰ These foundational beliefs about the ability of biometric data to uniquely identify an individual are not stable and are today highly contested. Research has demonstrated vulnerabilities as people age, and the inaccuracies that creep in when these systems are used to identify people of color, young and old people, manual laborers, those who speak English with a non-native accent, and many other demographic and phenotypic subgroups.¹¹ Biometric regulation does not interrogate these questions, but simply takes these claims of accuracy and equivalence to real identity as given.⁵

In data-protection laws, fulfilling the definition of “biometric data” or “biometric information” is the threshold condition for legal protections to apply. It also determines the stage (for, e.g., collection, processing, storage, and use) at which these protections are activated. When part of a broader personal data-protection law like the GDPR, such definitions usually work to distinguish biometric data from other kinds of personal data in order to offer special or stricter levels of protection. In laws like BIPA, which is solely focused on biometric data, the definition determines the scope of the legislation as a whole. Laws that establish government biometric ID projects, on the other hand, have tended toward an expansive definition that allows agencies to expand on the kinds of biometric data they can collect. The Kenyan draft law¹² and the Indian Aadhaar legislation¹³ list a series of identifiers that are currently collected under the project but allow the government to add to these categories of data collected at will.⁶

⁹ Article 4(14), GDPR.

¹⁰ Section 10, BIPA.

¹¹ See footnotes 34 and 35 of this compendium’s Introduction.

¹² The Huduma Namba Bill, 2019 defines biometric data as follows: “(B)‘biometric data’ includes fingerprint, hand geometry, earlobe geometry, retina and iris patterns, toe impression, voice waves, blood typing, photograph, or such other biological attributes of an individual obtained by way of biometrics.”

¹³ The Aadhaar Act, 2016 defines biometric information as follows: “‘biometric information’ means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.”

As legislation moves beyond traditional data privacy and security concerns to questions of accountability around whether or how to use these systems, and who is liable if these systems fail, some recent bills shift the focus from “data” to “systems.” For example, recent US legislation that restricts the use of these technologies does not define biometric data at all, and instead focuses on “face recognition systems” or “services,”¹⁴ or face/biometric “surveillance systems” as the object of regulation.¹⁵ The definitions of these terms emphasize the eventual uses or intentions that drive the application of such systems in social contexts (such as surveillance, identification, verification, or tracking).

The legal definition of biometric data is usually restricted to data that has been technically processed for use in an algorithmic system by specifying a particular digital representation (e.g., “template” or “print”). The definition often explicitly excludes photographs and voice recordings and creates a loophole around foundational stages when data is collected, processed, and stored.

The definition of biometric data has generally been restricted to mean a technically defined digital representation of bodily traits that have already been processed for machine or algorithmic analysis. This is suggested by semi-technical terms like “templates,” “geometry,” “prints,”¹⁶ or, in the GDPR, data that has already been subject to “specific technical processing.” Terms like “template” refer to the initial stage of algorithmic processing where data is extracted from, say, an image or voice recording. Modern machine learning systems do not need “all” of the data, but instead rely on extracting meaningful subparts from voice or image data, which can then be easily compared to existing “templates” in a database.¹⁷ This is the logic that leads to photographs of faces being expressly excluded from the definition of biometric data in the BIPA¹⁸ and the GDPR.¹⁹

14 Recent US legislation uses terms like “facial recognition systems,” as in the City of Boston Ordinance Banning Face Surveillance Technology, <https://www.eff.org/document/ordinance-banning-face-surveillance-technology-boston>; “facial recognition services,” as in the Washington Senate Bill 6280, is defined as “technology that analyzes facial features and is used by a state or local government agency for the identification, verification, or persistent tracking.” See SB 6280 (2019–20), <https://app.leg.wa.gov/billssummary?BillNumber=6280&Year=2019&Initiative=false>.

15 The phrase “face surveillance systems” appears in S.4084 (Facial Recognition and Biometric Technology Moratorium Act) introduced in June 2020, <https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-and-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology>. The term “biometric surveillance systems” is used in the California A.B. 1215 that bans face recognition on body-worn cameras; the bill refers to “any computer software or application that performs facial recognition or other biometric surveillance.”

16 See, for example, the way biometric data is defined in BIPA and other state biometric privacy laws, which specify “facial geometry,” “voice prints,” and “fingerprints.”

17 Kelly Gates, “Introduction: Experimenting with the Face,” in *Our Biometric Future* (New York: New York University Press, 2011).

18 Several defendants sued under BIPA have unsuccessfully argued before the courts that the specific exclusion of photographs means that information derived from photographs should also be excluded. In *Rivera v. Google, Inc.* (238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017), Google argued that its facial templates were derived from photographs, and therefore excluded from BIPA’s definition of biometric information, but the court held that templates were still biometric identifiers, since BIPA does not qualify the definition of biometric identifiers based on how they were derived. See Matthew T. Hays, “Technology Defendants Continue to Test Whether the Illinois BIPA Law Can Cope with Modern Facial Recognition Technology,” *Firewall*, December 6, 2019, <https://www.thefirewall-blog.com/2019/12/technology-defendants-continue-to-test-whether-the-illinois-bipa-law-can-cope-with-modern-facial-recognition-technology/>.

19 Recital 51 of the GDPR notes that “[t]he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.”

This narrow technical definition of biometric data creates a set of troubling loopholes. In her chapter, Els Kindt explains that the exclusion of photographs, voice recordings, or other forms of so called “raw” biometric data adversely limits the impact of the GDPR. She argues that heightened protections, like explicit consent, are foregone in the initial stage of data collection and storage (such as when a photo is uploaded to a social media site) and that use of such data without consent is often permitted by particular exceptions for law enforcement agencies after such data has been collected. ¹

The exclusion of photographs and voice recording is also troubling given the realities of how commercial and government surveillance systems are developed and deployed today. The harvesting of face images matched to individual names from the web is a common method used to create face-name databases. These databases are the foundation of sophisticated and covert surveillance tools created by private firms, who often do so in secret and proceed with almost no oversight.²⁰ The same covert surveillance practices are emerging with voice recordings.²¹ ²

The definition of biometric data offered in the California Consumer Protection Act (CCPA) of 2018 stands apart from existing definitions and could be instructive as a way to close this loophole. Rather than the current representation of the data, CCPA's definition focuses on *the ability to extract an identifier template* that can be algorithmically processed in order to determine whether it falls within the scope of the law.²² ³

Why have data-protection laws had limited effectiveness in curbing the expansion of biometric surveillance infrastructure by government? ⁴

Principles of data minimization and purpose limitation have rarely been applied to challenge the creation or expansion of biometric systems. Rather than an evidence-based scrutiny of the link between the means and the ends, the broad rationale of security and efficiency in service delivery has usually served to enable rather than restrict the use of biometric systems. ⁵

²⁰ 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/>; and Louise Matsakis, “Scraping the Web Is a Powerful Tool. Clearview AI Abused It,” Wired, January 25, 2020, <https://www.wired.com/story/clearview-ai-scraping-web/>.

²¹ Jeremy Kirk, “Hey Alexa. Is This My Voice or a Recording?,” BankInfoSecurity, July 6, 2020, <https://www.bankinfosecurity.com/hey-alexa-this-my-voice-or-recording-a-14562>; George Joseph and Debbie Nathan, “Prisons across the U.S. 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/>.

²² See Section 3(e) of the CCPA of 2018: “Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, *from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted...*” (emphasis mine).

Necessity and proportionality are common legal principles in international human rights law and reflected in a number of data-protection laws across the world.²³ They require that any infringement of privacy or data-protection rights be necessary and strike the appropriate balance between the means used and the intended objective. The proportionality principle is also central to constitutional privacy case law across the world, and while there are regional differences, these tests generally involve a balancing exercise where the right to privacy is balanced against a competing right or public interest.²⁴

In data-protection regulation, these principles are reflected in the types of data categories that are collected,²⁵ how the data can be used,²⁶ and how long it can be stored.²⁷ Under the GDPR and similar data-protection laws, the “data minimization” provision in Article 5 requires that entities limit personal data collection to that which is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.” For law enforcement agencies, the Data Protection Law Enforcement Directive (DP LED) requires a higher standard of whether that biometric data collection is “strictly necessary.”²⁸

Taken seriously, these provisions question whether the collection of biometric data is necessary in the first place.²⁹ For example, the Swedish Data Protection Authority outlawed the use of facial recognition in schools on the grounds that its use for attendance was a disproportionate means to achieve this goal when far less intrusive means exist.³⁰ The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*, or CNIL) and the regional court of Marseille also ruled similarly to declare the trial of facial recognition attendance systems illegal in France.³¹

In Ben Hayes and Massimo Marelli’s chapter, they explain how the International Committee of the Red Cross (ICRC) applied data-protection proportionality principles to the use of biometrics for aid distribution to people in need of humanitarian assistance. While the ICRC eventually determined that there was a “legitimate interest” in using biometric systems for this purpose, they limited the use to a “token-based system” (i.e., a card on which people’s biometric data is securely stored). The ICRC decided not to collect, retain, or further process people’s biometric data, and therefore not to establish a biometric database. If people want to withdraw or delete their biometric data, they can either return the card or destroy it themselves.

23 See Privacy International, “Towards International Principles on Communications Surveillance,” November 20, 2012, <https://privacyinternational.org/blog/1360/towards-international-principles-communications-surveillance>. The article refers to a meeting of experts in Brussels in October 2012. See also European Data Protection Supervisor, “Necessity & Proportionality,” n.d., https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. See generally Charlotte Bagger Tranberg, “Proportionality and Data Protection in the Case Law of the European Court of Justice,” *International Data Privacy Law* 1, no. 4 (November 2011): 239–248, <https://doi.org/10.1093/idpl/ipr015>.

24 See generally Alec Stone Sweet and Jud Mathews, “Proportionality Balancing and Global Constitutionalism,” *Columbia Journal of Transnational Law* 47, no. 72 (2008–09): 112.

25 See Article 5(c), GDPR on “data minimization,” and Article 9, GDPR on processing of special categories of personal data.

26 See Article 5(b), GDPR on “purpose limitation.”

27 See Article 5(e), GDPR on “storage limitation.”

28 See Article 10, DP LED on processing of “sensitive categories” of personal data.

29 See Els Kindt, “Biometric Applications and the Data Protection Legislation: The Legal Review and the Proportionality Test,” *Datenschutz und Datensicherheit* 31, no. 3 (2007): 166–170, https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/880dud3-2007-1662f90.pdf. See also Yue Liu, “The Principle of Proportionality in Biometrics: Case Studies from Norway,” *Computer Law & Security Review* 25, no. 3 (December 2009): 237–250.

30 Sofia Edvardsen, “How to Interpret Sweden’s First GDPR Fine on Facial Recognition in School,” IAPP, August 27, 2019, <https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/>.

31 EDRi, “Ban Biometric Mass Surveillance,” May 13, 2020, <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>.

Unfortunately, the application of these principles to challenge the creation of biometric systems and databases is rare, especially during the key initial or “pilot” stages before these systems are built and used.³² More often than not, inquiries into “necessity” are structured to enable rather than restrict the use of biometric systems. Even where data minimization principles exist, the notoriously broad but powerful rationale of “efficiency” or “law and order” and “national security” serve to grant most government uses of biometrics a free pass without any evidence-based scrutiny of the relationship between means and ends.³³ As noted in the European Digital Rights (EDRi) 2020 report on biometric mass surveillance, this uneven application of the law can also be attributed to the European Union’s inadequately resourced and politically disempowered National Data Protection Authorities. On the other hand, in countries that still lack data-protection laws and data-protection authorities (DPAs), when biometric ID projects have faced constitutional challenges in the Court, the proportionality test is often overlooked in favor of broad claims around the efficiency of biometric service delivery systems, with scant analysis of alternative, less rights-infringing means to achieve that goal.³⁴

1

Legal principles of “purpose limitation” are often ineffective given the broader political and institutional trends working to dissolve boundaries between civilian, criminal, and immigration biometric databases. Driver’s license face databases are a key site for this kind of “function creep” and require urgent policy intervention.

2

The “purpose limitation” principle restricts the use of data for purposes beyond what it was originally collected for; a specified purpose must not be used for another “incompatible” purpose. Yet pervasive “security” imperatives often blur the boundaries between criminal, welfare, and immigration processes and, consequently, obfuscate what is perceived and understood as a “compatible” purpose. Under the US federal Secure Communities program (S-COMM), states submit fingerprints of arrestees to criminal as well as immigration databases, allowing Immigration and Customs Enforcement (ICE) to access this information.³⁵ ICE has also requested face recognition searches of driver’s license databases in multiple states in the US.³⁶ In Australia, the Home Affairs department has been centralizing state driver’s license face databases to use for broader policing and law enforcement purposes.³⁷ India’s biometric ID project Aadhaar is

3

32 See EDRi, “Evidence on Biometrics and Fundamental Rights,” July 2020 (submitted to the European Commission consultation and on file with the author) for a list of projects, including multiple case studies from Europe that were not properly assessed due to the claim that they were in the “experimental” or “pilot” stage.

33 In the European context, see Fundamental Rights Agency (FRA), “Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement,” 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf. The authors note that “[a]n objective of general interest—such as crime prevention or public security—is not, in itself, sufficient to justify an interference” with fundamental rights, meaning that the Law Enforcement Directive’s data protections must apply.

34 See Mariyan Kamil, “The Aadhaar Judgment and the Constitution – II: On Proportionality,” *Indian Constitutional Law and Philosophy*, September 30, 2018, <https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/>.

35 As a result of this, anyone arrested for a state crime (even if they were never charged or were wrongly arrested) is vulnerable to deportation or detention. See Jennifer Lynch, “From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond,” *American Immigration Council*, May 23, 2012, <https://www.americanimmigrationcouncil.org/research/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond/>; see also ACLU, “Secure Communities (‘S-Comm’),” n.d., <https://www.aclu.org/other/secure-communities-s-comm>.

36 Harrison Rudolph, “ICE Searches of State Driver’s License Databases,” *Center on Privacy & Technology at Georgetown Law*, Medium, July 8, 2019, <https://medium.com/center-on-privacy-technology/ice-searches-of-state-drivers-license-databases-4891a97d3e19>.

37 See Jake Goldenfein and Monique Mann, “Australian Identity-Matching Services Bill,” in this compendium.

widely known as a welfare delivery system, yet government officials may use the data for national security purposes in limited circumstances,³⁸ and the National Crime Bureau has publicly stated their desire to use the system for criminal investigations.³⁹ These systems are *structured* to evade and remove the purpose limitations on data use.

The failure of proportionality safeguards is also borne out in the context of centralized biometric ID systems where legislation has frequently been introduced only after these systems are developed, and in some cases after they're already deployed and in use.

Large-scale biometric ID projects that span welfare, criminal, and immigration contexts have typically been implemented as technocratic exercises driven by executive agencies, often with the glaring absence of law. Even as advocacy efforts focus on demanding legal frameworks to ensure legislative and public scrutiny, legislation often comes too little, too late. For one, many projects do not receive proper scrutiny or are passed through extraordinary measures that forgo scrutiny altogether.⁴⁰ In other cases, weak procedural safeguards are proposed, but the broader centralization of power in a few agencies remains unchallenged.

In Jake Goldenfein and Monique Mann's chapter, they argue that the Australian Identity Services Bill provided the Home Affairs department with authorization to become the central node ("the hub") through which all identity and suspect identification requests would be routed. They conclude that "a true proportionality analysis" might have questioned whether a centralized facial recognition database was in fact necessary to address the stated purpose of curbing identity fraud, but in reality "this framing is operationalized in ways that enable continuing expansion of surveillance systems."

The mere existence of procedural safeguards like data security or consent can obscure the root of the problem, only serving to legitimize the continued existence of these systems. When faced with existential threats, like the potential of being invalidated by the highest courts, data-privacy rules have repeatedly been held up as an adequate safeguard against the concerns raised, leading to widespread skepticism about the role these laws play.⁴¹ In the case of India's nationwide biometric ID project (Aadhaar), legislation authorizing and regulating the project came nearly a decade after biometric data collection began. This massive delay is even more concerning given the absence of a data-privacy law that applied to government agencies. In her contribution to this compendium, Nayantra Ranganathan challenges foundational assumptions about the role of the

38 Vrinda Bhandari and Renuka Sane, "A Critique of the Aadhaar Legal Framework," *National Law School of India Review* 31, no. 4 (2019):1–23.

39 Aman Sharma, "Cannot Share Aadhaar Biometric Data for Crime Investigations," *Economic Times*, June 22, 2018, <https://economictimes.indiatimes.com/news/politics-and-nation/cannot-share-aadhaar-biometric-data-for-crime-investigations-uidai/articleshow/64700379.cms>.

40 See Nayantra Ranganathan's chapter in this compendium, "The Economy (and Regulatory Practice) That Biometrics Inspires: A Study of the Aadhaar Project," in which she describes the truncated and legally dubious passage of the Aadhaar as a "money bill." See also ADC, "ADC Files an Action of Unconstitutionality before GCBA after the Introduction of Face Recognition System," November 6, 2019, <https://adc.org.ar/en/2019/11/06/adc-files-an-action-of-unconstitutionality-before-gcba-after-the-introduction-of-face-recognition-system/>.

41 See commentary on the Kenyan data-protection law by Rasna Warah, "Data Protection in the Age of Huduma Namba: Who Will Benefit?," *Elephant*, November 29, 2019, <https://www.theelephant.info/op-eds/2019/11/29/data-protection-in-the-age-of-huduma-namba-who-will-benefit/>; and see Praavita, "Can the Aadhaar Act and a Data Protection Act Coexist?," *The Wire*, July 30, 2018, <https://thewire.in/law/can-the-aadhaar-act-and-a-data-protection-act-coexist>.

law in relation to these projects, characterizing regulation as a legitimizing force that reflects the interests of the powerful actors that drive these systems. She argues that Aadhaar's regulation functioned to "consolidate the developments of the first seven years of the project, and also presented a revisionist history of the actual goals of the project, obscuring the stakes for private interests...[M]any of the problems with Aadhaar should not be understood as failures of law or regulation, but products of law and regulation."

Is meaningful notice and consent possible in the context of biometric systems? What are the limitations of a consent-based approach and what supplements or alternatives might be required?

Given the predominance of the data-protection approach, notice and consent has been a cornerstone of biometric regulation, yet the well-documented limitations of this model underscore the need for additional necessity and proportionality limits even after consent has been obtained. Recent AI legislation also requires broader "explainability" requirements as a core component of meaningful notice.

While notice and consent has traditionally been the cornerstone of data-protection and privacy approaches globally, its limitations have been laid bare in recent years, leading to skepticism about (if not outright rejection of) the idealized conception of "individual control."⁴² In their chapter, Ben Hayes and Massimo Marelli explain why the Red Cross removed consent as a legal "ground of processing"⁴³ in emergency humanitarian contexts where, the authors argue, consent can never be assumed to be "freely given."

At the same time, the individual's right to refuse or revoke permission for the collection or use of their data has been an important tool in challenging biometric systems like live facial recognition in public spaces that are designed to evade such active permission. As described in Woodrow Hartzog's chapter, under BIPA, the failure to obtain consent from individuals before using their biometric data has led to several successful lawsuits against some of the largest tech companies in the world and is the basis for the lawsuit recently launched against Clearview AI.⁴⁴

42 For a rejection of the idea of privacy as "control," see generally Ruth Gavison, "Privacy and the Limits of Law," *Yale Law Journal* 89, no. 3 (January 1980): 421–471. See also Woodrow Hartzog, "The Case Against Idealising Control," *European Data Protection Law Review* 4, no. 4 (2018): 423–432.

43 *Grounds of processing* is a legal term of art popularized by the GDPR. It refers to a number of legal justifications, of which at least one must be met in order to "process" (i.e., collect, store, use, etc.) personal data. Grounds of processing include consent, performance of a contract, legitimate interests of a business, and so on.

44 Woodrow Hartzog, "BIPA: The Most Important Biometric Privacy Law in the US?," in this compendium.

In the GDPR, consent is supplemented by several general limits of proportionality and necessity⁴⁵ 1 that hold irrespective of whether consent is obtained. By contrast, US state laws like BIPA focus on notice and consent with few additional restrictions on collection or use beyond the prohibition against selling biometric data for profit and limits on retention.

As Hartzog concludes, BIPA has done “very little to bring about the kind of structural change and substantive limits necessary.” For one, he explains how most of us are simply “not capable of meaningfully exercising our agency over modern data practices” and argues that BIPA provides little protection from the “post-permission risks” of biometric technologies.⁴⁶ This underscores the need for additional transparency and accountability, including bright-line restrictions alongside a robust notice and consent regime. 2

Emerging regulatory approaches for algorithmic or AI systems include a broader understanding of notice that goes beyond simply informing the individual that algorithmic tools are being used. These newer approaches also take into account how these systems work, the context in which these systems are used, and what criteria are informing algorithmic decisions. This broad scope will be especially valuable in regulating biometric systems that serve purposes beyond identification and verification. The Illinois Artificial Intelligence Video Interview Act is an example of a notice provision tailored to the specific context of job interviews; it requires that all job applicants be informed when AI systems used to assess their performance as a candidate are deployed during interviews. In addition to this, it requires that each applicant be provided clear information about “how the artificial intelligence works and what general types of characteristics it uses to evaluate applicants.”⁴⁷ Whether such explanations are possible, and whether they can work to inform meaningful choices on the part of job seekers given the power dynamics at work in the context of a job interview, have yet to be seen. 3

45 See Article 5 GDPR including principles of data minimization, collection limitation, purpose limitation, storage limitation principles.

46 Ibid.

47 See Section 5, “Artificial Intelligence Video Interview Act,” <http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101-0260>.

SECTION 2. BEYOND PRIVACY: ACCURACY, DISCRIMINATION, HUMAN REVIEW, AND DUE PROCESS¹

How should regulatory frameworks address concerns about accuracy and non-discrimination in biometric systems?²

To what extent should regulation rely on standards of performance and accuracy set by technical standards-setting bodies?³

*While accuracy and discrimination concerns are at the forefront of public debate, corresponding legal protections have been rare in existing regulatory frameworks. However, recent legislation and advocacy efforts in the US have mandated accuracy and nondiscrimination audits for facial recognition systems, going as far as to require such audits as a condition for lifting a moratorium on use.*⁴

*While technical standards (e.g., NIST's Face Recognition Vendor Test) are evolving to account for bias and inaccuracy, they generally underperform in "real-life" contexts and are limited in their ability to address the broader discriminatory impact of these systems as they are applied in practice. If such standards are positioned as the sole check on facial recognition systems, they could function to obfuscate, rather than mitigate, harm.*⁵

Accuracy and "error rates" metrics are a staple of the mainstream conversations around biometrics and are used as a tool in the machine learning field to compare systems and assess progress. Accuracy claims have been a simple way for those developing, marketing, and applying these systems to "prove" effectiveness, and to demonstrate that automation offers an improvement over manual processes. In the past two years, however, the same facial recognition systems that boast high accuracy rates according to such narrow metrics have been shown to perform less well when accuracy rates are stratified across demographics like age, race, gender, and disability.⁴⁸ "Errors" in these systems are not evenly distributed, and reflect historical

48 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>.

patterns of racism, gender bias, and ableist discrimination. To remedy this problem, researchers have called for auditing on accuracy across specific demographic and phenotypic subgroups, accompanied by measures that can close performance gaps where they arise.⁴⁹

To accomplish such audits, many are turning to technical standard-setting bodies that set benchmarks for accuracy, performance and safety. Auditing protocols like the National Institute of Standards and Technology (NIST) 2019 Face Recognition Vendor Test (part three) evaluate whether the algorithm performs differently across different demographics in the dataset.

Regulators and lawmakers have also begun to take notice, calling for audits by technical standards-setting bodies that set benchmarks for accuracy, performance, and safety. In March 2020, the UK Equality and Human Rights Commission called to suspend the use of facial recognition in England and Wales until discrimination against protected groups has been independently scrutinized. Recent legislation in the US includes accuracy and nondiscrimination audits as a condition for the use of facial recognition. The Washington State Bill SB 6280, passed in March 2020, requires that face recognition companies cooperate to allow for independent testing for “accuracy and unfair performance” across subgroups including race, skin tone, ethnicity, gender, age, or disability status. If independent testing reveals “material unfair performance differences,” companies are required to rectify the issues within ninety days. Another proposed federal bill (S.2878: the Facial Recognition Technology Warrant Act of 2019) requires federal law enforcement agencies to work with NIST⁵⁰ to establish testing systems to ensure consistent accuracy across gender, age, and ethnicity.

While these standards are a step in the right direction, it would be premature to rely on them to assess performance, and they do not adequately capture the broader discriminatory impacts these systems might have when they are used. First, researchers and advocacy organizations have found that many of the systems that “pass” current benchmark evaluations continue to underperform in real-life contexts.⁵¹ Additionally, there is currently no standard practice to document and communicate the histories and limits of benchmarking datasets, and thus no way to determine their applicability to a particular system or suitability for a given context.

Moreover, creating a solely technical threshold to judge discriminatory impact can distort the biased practical implementation of these technologies and their weaponization against specific groups. For example, facial recognition systems are deployed disproportionately in minority communities, so even the most accurate systems will be discriminatory. They also “run the risk of providing ‘checkbox certification,’ allowing vendors and companies to assert that their technology is safe and fair without accounting for how it will be used, or its fitness for a given context.”⁵²

49 See Raji and Buolamwini, “Actionable Auditing,” and Buolamwini et al., Gender Shades, MIT Media Lab, <http://gendershades.org>.

50 NIST is a non-regulatory federal agency within the US Department of Commerce. Its mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Auditing protocols like the NIST 2019 Face Recognition Vendor Test (part three) evaluate whether the algorithm performs differently across different demographics in the dataset.

51 See Inioluwa Deborah Raji and Genevieve Fried, “About Face: A Survey of Facial Recognition Evaluation,” Meta-Evaluation workshop at AAAI Conference on Artificial Intelligence (forthcoming, 2020); Pete Fussey and Daragh Murray, “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology,” The Human Rights, Big Data and Technology Project, July 2019, <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>.

52 Written Testimony of Meredith Whittaker, US House of Representatives Committee on Oversight and Reform, “Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy, January 15, 2020, <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/WRITTEN%20testimony%20-%20MW%20oversight.pdf/>.

Does requiring “meaningful human review” of biometric recognition systems ensure oversight and accountability?¹

Recent legislation includes provisions that mandate “meaningful human intervention”² in the results of biometric systems. However, a large body of research suggests that the people who review the results of biometric systems overwhelmingly overestimate credibility, and often respond inaccurately and with bias.

“Human intervention” in automated decisions has gained considerable acceptance as a legal approach to provide a meaningful check on the potential harms these systems represent. Article 22 of the GDPR, for example, includes a restriction on “solely automated decisions,” and requires human intervention when automated systems impact “legal or similarly significant” decisions about people’s lives. The recently passed and heavily criticized⁵³ Washington State facial recognition law similarly includes provisions for “meaningful human review” and periodic officer training as conditions for the use of biometric technology. Human review is defined in terms of “review or oversight by one or more individuals...who have the authority to alter the decision under review.”⁵⁴

However, a large body of research demonstrates that human intervention in these systems does not address major concerns about transparency or control. Individuals who review results are often unable to accurately evaluate the quality or fairness of the outputs, and often respond to predictions in biased and inaccurate ways.⁵⁵ The ACLU has pointed to the imprecisely defined notion of meaningful human review as “deeply flawed” given its vague definition. They maintain that it should not become a rubber stamp that allows for the use of facial recognition or similar systems in sensitive social domains like welfare and criminal justice.⁵⁶

In their chapter, Peter Fussey and Daragh Murray show that human operators who assess live facial recognition “matches” often defer to the algorithm’s output, despite the known inaccuracy of such output—a phenomenon referred to as “automation bias.” In their research, they found that “humans overwhelmingly overestimated the credibility of the system.”⁵⁷ The Indian government established a system of “manual overrides” to address the issue of biometric errors that lead to

53 Jennifer Lee, “We Need a Face Surveillance Moratorium, Not Weak Regulations: Concerns about SB 6280,” ACLU, March 31, 2020, <https://www.aclu-wa.org/story/we-need-face-surveillance-moratorium-not-weak-regulations-concerns-about-sb-6280>.

54 Section 2(7), Washington Senate Bill 6280, <http://lawfilesexternal.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729>.

55 See Ben Green and Yiling Chen, “Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments,” January 2019, <https://www.benzevgreen.com/wp-content/uploads/2019/02/19-fat.pdf>; Ben Green and Yiling Chen, “The Principles and Limits of Algorithm-in-the-Loop Decision Making,” November 2019, <https://www.benzevgreen.com/wp-content/uploads/2019/09/19-cscw.pdf>; Megan Stevenson, “Assessing Risk Assessment in Action,” *Minnesota Law Review* 103, no. 303 (2018), <https://dx.doi.org/10.2139/ssrn.3016088>; Berkeley J. Dietvorst, Joseph P. Simmons, and Cade Massey, “Algorithm Aversion: People Erroneously Avoid Algorithms after Seeing Them Err,” *Journal of Experimental Psychology* 144, no. 1 (February 2015): 114–126, <https://psycnet.apa.org/fulltext/2014-48748-001.html>; Amirhossein Kiani et al., “Impact of a Deep Learning Assistant on the Histopathologic Classification of Liver Cancer,” *npj Digital Medicine* 3, no. 23 (2020), <https://doi.org/10.1038/s41746-020-0232-8>.

56 Lee, “We Need a Face Surveillance Moratorium.”

57 See Peter Fussey and Daragh Murray, “Policing Uses of Live Facial Recognition in the United Kingdom,” in this compendium.

exclusion from government benefits and systems.⁵⁸ However, studies suggest that even these legal norms did not always govern the behavior of those operating the biometric systems on the ground. Those managing these systems often failed to exercise this option and refused people access to services because of “‘incorrect’ (or rather complete lack of) human intention in overcoming technological failure.”⁵⁹

An open question for future legal approaches is how to incentivize and ensure real capacity for human oversight. This would include an assessment of the gaps in knowledge, biases, or inefficiencies that limit accountability and prevent human operators from assessing or anticipating problems with these systems.

Should regulatory frameworks create a risk-based classification between “identification” and “verification” uses of biometric recognition?

What are the potential risks of a permissive regulatory approach to verification?

Recent official policy documents in the EU suggest that “verification” (1:1) is an inherently less risky use compared to identification (1:n) in terms of accuracy, data security vulnerabilities, and the capacity for meaningful consent.

However, any broad-brush permissive approach to verification in the law should be avoided. Even if participation in a verification system is with knowledge, these systems might not afford individual’s real choice when they act as gatekeepers to access essential spaces or services.

The distinction between verification and identification is often described in terms of the technical shorthand 1:1 versus 1:n. 1:1 verification (or authentication) aims to determine whether people are who they claim to be through a one-to-one match that queries biometric information (e.g., a facial scan by a smartphone) against the data that the person has previously provided (e.g., the person stores their photograph on the phone when they first purchase it).⁶⁰ Identification, or 1:n, is a more technically involved process that compares the biometric information of an

58 Ronald Abraham et al., “State of Aadhaar Report 2017–18,” IDinsight, May 2018, https://static1.squarespace.com/static/5b7cc54eec4eb7d25f7af2be/t/5bbd2874c8302561862f03d4/1539123330295/State+of+Aadhaar+Report_2017-18.pdf.

59 See Bidisha Chaudhuri, “Paradoxes of Intermediation in Aadhaar: Human Making of a Digital Infrastructure,” *Journal of South Asian Studies* 42 (2019): 572–587, <https://doi.org/10.1080/00856401.2019.1598671>.

60 See Stan Z. Li and Anil K. Jain, *Handbook of Face Recognition* (New York: Springer, 2005), 1–15.

unknown person against a database of many people's biometric data. An algorithm determines if the person is represented in the database and who they might be. Some identification systems provide a number of "similar faces" that meet a specified confidence or accuracy threshold.⁶¹ 1

Recent official policy documents⁶² as well as data-protection authorities in the EU⁶³ suggest that verification is an inherently less risky use of biometrics in terms of accuracy, data security vulnerabilities, and the capacity for meaningful consent. Biometric locks on phones are a common example used to demonstrate these claims, and San Francisco recently amended its facial recognition moratorium to allow employees to use biometric lock features on government-issued cell phones.⁶⁴ By contrast, some of the most controversial reported cases of facial recognition largely pertain to identification (1:n) systems like live facial recognition (LFR), which has a record of high error rates. 2

These accounts of verifications often link or even conflate the claim of higher accuracy with meaningful consent. The claim is that with verification systems, people are willing to present their biometrics in a "cooperative" way (like a frontal face with eyes open), whereas with identification, people could be unaware of being identified, which increases the error rates.⁶⁵ Any general assumption that verification systems involve the active and targeted participation of the individual, however, rests on shaky foundations. While these systems might have higher accuracy rates than identification systems, they are still predictive and not immune to the same kinds of errors and biases across lines of race, gender, and other demographic traits. More importantly, even if participation is done with volition and knowledge, these systems might not afford individuals real choice when they act as gatekeepers to access to essential spaces and services. This became a focal point in the opposition against biometric ID systems in India and Kenya,⁶⁶ as well as in the use of biometric systems in humanitarian contexts.⁶⁷ 3

61 Ibid.

62 See Luana Pascu, "New EU AI Strategy Puts Remote Biometric Identification in 'High-Risk' Category," *BiometricUpdate.com*, February 19, 2020, <https://www.biometricupdate.com/202002/new-eu-ai-strategy-puts-remote-biometric-identification-in-high-risk-category>; Paul de Hert and Koen Christianen, "Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data," Tilburg Institute for Law, Technology, and Society, April 2013, <https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81>; see also, e.g., Article 29—Data Protection Working Party, "Working Document on Biometrics (WP 80)," 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf; "Opinion 02/2012 on Facial Recognition in Online and Mobile Services (WP192)," March 23, 2012, <https://www.pdpjournals.com/docs/87997.pdf>; and "Opinion 3/2012 on Developments in Biometric Technologies (WP193)," April 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf; and see CNIL, "Facial Recognition: For a Debate Living Up to the Challenges," December 19, 2019, <https://www.cnil.fr/en/facial-recognition-debate-living-challenges>.

63 See French data-protection authority CNIL, *Communication central storage fingerprint*, 2007; and cf. Els Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Dordrecht: Springer, 2013), 540.

64 Tim Cushing, "San Francisco Amends Facial Recognition Ban after Realizing City Employees Could No Longer Use Smartphones," *Techdirt*, December 20, 2019, <https://www.techdirt.com/articles/20191219/18253743605/san-francisco-amends-facial-recognition-ban-after-realizing-city-employees-could-no-longer-use-smartphones.shtml>.

65 See Li and Jain, *Handbook of Face Recognition*, 1–15.

66 Abdi Latif Dahir and Carlos Mureithi, "Kenya's High Court Delays National Biometric ID Program," *New York Times*, January 31, 2020, <https://www.nytimes.com/2020/01/31/world/africa/kenya-biometric-id-registry.html>; see also reportage on the farcical nature of "consent camps" for Aadhaar discussed during the People's Tribunal on Aadhaar-related Issues, February 28, 2020, <https://threadreaderapp.com/thread/1233608762604154880.html>.

67 Petra Molnar, "The Contested Technologies That Manage Migration," CIGI Online, December 14, 2018, <https://www.cigionline.org/articles/contested-technologies-manage-migration>.

Proponents of permissive approaches to verification typically argue that these systems involve local data storage, which minimizes the data security risks that come with centralized databases. However, access control at borders, airports, and buildings often centralize biometric authentication systems for access to services, and many of these systems maintain centralized storage and authentication records.⁶⁸ Risks associated with biometric use are certainly contextual, but any broad-brush permissive approach to verification in the law should be avoided, especially where it can create loopholes that allow more harmful implementations of verification.

What kinds of due process safeguards are required for law enforcement use of biometric recognition?

Should law enforcement have access to these systems to begin with?

Outside of a complete ban on law enforcement use, recent regulatory approaches have focused on strengthening due process safeguards. This includes requiring warrants for ongoing surveillance, restricting the use of facial recognition to serious crimes, and ensuring defendants get meaningful access to biometric evidence that is used against them.

While facial recognition has received special regulatory attention, these tools should be understood as part of a broader set of algorithmic police surveillance tools, including drone surveillance, license plate recognition, and predictive policing.

The use of biometric technologies in policing raises a range of legal issues, many of which have been debated and litigated over the years in the context of fingerprinting and DNA.⁶⁹ These include the conditions under which biometric data can be taken (whether it should be at arrest or upon conviction), and the circumstances under which it should be deleted from such databases (for example, if a person is never convicted or if a conviction is overturned). The increasing shift to use of face and voice identifiers has exacerbated some of these existing concerns and created new ones. Indeed, law enforcement use of facial recognition has been the subject of intense public and regulatory scrutiny recently. These systems have misidentified people and been disproportionately used to target communities of color. Moreover, the vast majority of cases involving face recognition searches are not disclosed, depriving defendants of the ability to challenge evidence that could determine their fate in criminal trials.⁷⁰

68 For an enumeration of concerns with centralized or centrally linked biometric ID infrastructures, see Access Now, #WhyID campaign, 2019, <https://www.accessnow.org/whyid/>.

69 See Robyn Caplan et al., "Data & Civil Rights: Biometric Technologies in Policing," *Data & Society*, October 27, 2015, <https://datasociety.net/library/data-civil-rights-biometric-technologies-in-policing/>; Brandon L. Garrett, "DNA and Due Process," *Fordham Law Review* 78, no. 6 (2010): 2919–2960; Elizabeth N. Jones, "Spit and Acquit": Legal and Practical Ramifications of the DA's DNA Gathering Program," *Orange County Lawyer Magazine* 51, no. 9 (September 2009), <http://papers.ssrn.com/sol3/papers.cfm?abstractid=1809997>.

70 See section on Florida case involving FACES facial recognition system used in the case against Willie E. Lynch in 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>.

Outside of complete bans, there are multiple proposals that seek to regulate different aspects of law enforcement use. In their chapter, Jameson Spivack and Clare Garvie outline emergent regulatory approaches in the US that focus on limiting the use of facial recognition. Some limitations are based on the seriousness of the crime (e.g., only for violent felonies), while others ban the use in conjunction with body cameras or drones. There are also bills that would require a court order to run facial recognition searches,⁷¹ as well as one that would require that defendants have access to source code and other information necessary to exercise their due process rights when algorithms are used to analyze evidence in their case.⁷²

1

While facial recognition has received special regulatory attention, these tools should be understood as part of a broader set of algorithmic surveillance tools, including drone surveillance, license plate recognition, and predictive policing.⁷³ These systems raise similar challenges for established principles around procedural fairness, such as notice, hearing, the disclosure of evidence, establishing reasons for decisions, and the ability to challenge these decisions.

2

Law enforcement use of live facial recognition (LFR) has been the subject of intense public and regulatory scrutiny. Advocacy demands range from requiring a specific authorizing law to calls to ban law enforcement use of LFR altogether.

3

Live facial recognition systems in public spaces are particularly controversial. Typically, cameras are deployed at a fixed location and the list of people who are identified is communicated to law enforcement officers on the ground.⁷⁴ Despite LFR's implications for privacy, criminal due process, and freedom of speech or expression, these tools have largely been rolled out without undergoing public and parliamentary scrutiny.

4

In their chapter, Peter Fussey and Daragh Murray describe London's expansive LFR program,⁷⁵ and discuss how the London Metropolitan Police successfully argued before the High Court that LFR was part of their inherent powers, and thus did not need new legislation to explicitly authorize its use.⁷⁶ The case is on appeal, but one of the factors that contributed to the Court's decision was the notion that LFR was not "invasive" technology and therefore did not require special sanction. Buenos Aires has also conducted an expansive LFR program.⁷⁷ In this case, the municipal government pushed through a resolution with truncated processes that authorized the use of these systems with minimal safeguards. Advocacy organizations have challenged the constitutionality of this ordinance.⁷⁸

5

71 See, e.g., the proposed Facial Recognition Technology Warrant Act Of 2019, <https://www.coons.senate.gov/imo/media/doc/FRTWA%20One-Pager%20FinalFinal.pdf>.

72 "H.R. 4368: Justice in Forensic Algorithms Act of 2019," <https://www.congress.gov/bill/116th-congress/house-bill/4368/text>.

73 See Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," ACLU, 2019, <https://www.aclu.org/report/dawn-robot-surveillance>.

74 LFR refers to facial recognition that is "always on," identifying people in real time as they move through public and private space.

75 Metropolitan Police UK, "Live Facial Recognition," n.d., <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/>.

76 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, 4 September 2019, para. 78. ("AFR Locate" is South Wales Police's nomenclature for LFR.)

77 Dave Gershorn, "The U.S. Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life," OneZero, Medium, March 4, 2020, <https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d>.

78 ADC, "ADC Files an Action of Unconstitutionality before GCBA."

Increasingly, privacy advocates are calling for a complete ban on LFR, viewing it as incompatible with fundamental rights and entailing risks that cannot be mitigated through procedural safeguards.¹

Are systems that process bodily data for purposes beyond establishing individual identity, like making inferences around emotional state, personality traits, or demographic characteristics, covered under existing biometric regulation?²

Should such systems be permitted at all, given their contested scientific foundations and mounting evidence of harm?³

*Since many emotion recognition and personality prediction systems rely on face and voice data that could be used to identify an individual (even if that is not its current purpose), these systems could fulfill the definitional threshold of data-protection laws like the GDPR. Many recent moratorium bills in the US include systems that infer “emotion, associations, activities, or the location of an individual.”*⁴

*However, many organizations are calling to ban these systems altogether given discredited scientific foundations and mounting evidence of harm.*⁵

It is unclear whether existing biometric regulation will apply to systems where the primary purpose is to infer emotional states, interior characteristics, or identities like gender, race, ethnicity, and age.⁷⁹ The fact that these systems rely on face or voice data that could be used to confirm or establish an individual’s identity (even if that is not its current purpose) could mean that these systems fulfill the definitional threshold of biometric data under data-protection laws like the GDPR. The European Digital Rights Initiative (EDRI) has also argued that biometric processing under the GDPR should be interpreted to include “detection of appearance, inferred behavior, predicted emotions or other personal characteristics.”⁸⁰⁶

79 Some technical literature uses the term “soft biometrics” to define the process of “categorizing information about bodily traits where a person may not be identified in the process.” See 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>.

80 Sarah Chander, “Recommendations for a Fundamental Rights-Based Artificial Intelligence Regulation,” EDRI, June 4, 2020, https://edri.org/wp-content/uploads/2020/06/AI_EDRIRecommendations.pdf.

Many recent moratorium bills in the US include systems that use facial data for broader inferences, such as inferring “emotion, associations, activities, or the location of an individual.”⁸¹ The 2019 moratorium bills introduced in New York⁸² and Washington⁸³ include any automated process by which characteristics of a person’s face are analyzed to determine “the person’s sentiment, state of mind, or other propensities including, but not limited to, the person’s level of dangerousness.” In specific contexts, these systems will require additional norms around explainability or transparency about how inferences are made, such as in the Illinois AI Videoconferencing Act 2019, which regulates the use of these tools in hiring.

81 E.g., Bill S.1385/H.1538. See ACLU Massachusetts, “Face Surveillance Moratorium,” n.d., <https://www.aclum.org/en/legislation/face-surveillance-moratorium>. See also Ed Markey, “Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology,” June 25, 2020, <https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology>; and Cory Booker, “Booker Introduces Bill Banning Facial Recognition Technology in Public Housing,” November 1, 2019, <https://www.booker.senate.gov/news/press/booker-introduces-bill-banning-facial-recognition-technology-in-public-housing>.

82 Bill A6787D, New York <https://www.nysenate.gov/legislation/bills/2019/a6787>.

83 Bill HB 2856, Washington, <https://app.leg.wa.gov/billsummary?BillNumber=2856&Year=2019&Initiative=false>.

SECTION 3. EMERGING REGULATORY TOOLS AND ENFORCEMENT MECHANISMS¹

What are the different types of “bans” and moratoria that have been passed in the US over the last few years?²

How can moratoria conditions be strengthened to ensure that eventual legislative or deliberative processes are robust?³

How will bans and moratoria on government use impact the private development and production of biometric systems?⁴

*Over the past few years, a wave of municipal legislation has sought to ban government use of facial recognition in the US, and some states have also proposed similar bills. Many of these bans focus on law enforcement use. While some large tech companies have come out in favor of regulation, they have consistently pushed back against bans, often favoring much less stringent approaches.*⁵

*The term “moratorium” is shorthand for a range of regulatory interventions with varying conditions for when the restrictions would be lifted—from straightforward time-bound goals for drafting and authorizing legislation to the establishment of deliberative, consultative processes. Some moratorium bills prescribe specific conditions to ensure the quality of the legislation and meaningful community participation in any deliberative process.*⁶

Many cities and states in the US have recently introduced legislation that bans government use of facial recognition, with a primary focus on law enforcement use.⁸⁴ These legislative interventions have played an outsized role in shaping the regulatory landscape by introducing a complete prohibition as a regulatory option against which other, less strict interventions will be compared. As Jameson Spivack and Clare Garvie point out in their chapter, advocates have been critical of weaker regulatory bills for “using up available political capital” and potentially undercutting demands for bans in the future.⁸⁵

⁸⁴ In their contribution to this compendium, Jameson Spivack and Clare Garvie track this legislative activity, noting that “[a]s of July 2020, the following municipalities had banned face recognition: Alameda, California; Berkeley, California; Boston, Massachusetts; Brookline, Massachusetts; Cambridge, Massachusetts; Easthampton, Massachusetts; Northampton, Massachusetts; Oakland, California; San Francisco, California; and Somerville, Massachusetts. A number of states proposed bans on face recognition during the 2019–2020 legislative session: Nebraska, New Hampshire, New York, and Vermont.”

⁸⁵ See Spivack and Garvie, “A Taxonomy of Legislative Approaches to Face Recognition in the United States,” in this compendium.

1 Some of the largest technology companies that develop and sell these systems to law enforcement have been deeply engaged in these legislative processes, often publicly championing the need for some “regulation” but simultaneously lobbying against moratoria and bans. For example, Microsoft celebrated Washington State’s SB 6280 (“Finally, progress on regulating facial recognition,” Brad Smith, the company’s general counsel, announced), only to face questions and criticisms about their involvement in pushing through a law that was considered weak by many organizations, and that effectively undercut a potential ban on government use.⁸⁶

2 Moratoria and bans are often used interchangeably, yet Spivack and Garvie argue that this shorthand conceals a wide spectrum of regulatory interventions. Moratoria, in particular, contain a range of approaches that vary widely in terms of strictness and the conditions for lifting restrictions. While some moratoria stop all use of face recognition for a predetermined time, there is a risk that the legislature fails to act before the period is over and facial recognition use recommences without any further legislative intervention. On the other hand, directive moratoria ban the use of facial recognition until a law is passed and/or a statutory body (e.g, a task force or committee) is formed to submit recommendations for what to include in the law.

3 Moratoria can work to fast-track a deliberative or legislative process where one might not otherwise have been possible. While this is welcome, it is also eventually susceptible to the vested public and private interests that will push for weak or no legislation. There is a risk that a task force created by these laws “may not be representative of affected communities; may lack authority; or may be inadequately funded.”⁸⁷ Some moratoria do more to prevent weak regulation than others. A 2019 Massachusetts law sets minimum requirements for what future legislation should achieve, including data privacy safeguards, auditing requirements, and protection for civil liberties. Similarly, the recently passed Washington State law specifies that the legislative task force be comprised of “advocacy organizations that represent consumers or protected classes of communities historically impacted by surveillance technologies including, but not limited to, African American, Hispanic American, Native American, and Asian American communities, religious minorities, protest and activist groups, and other vulnerable communities.”⁸⁸

86 See Dave Gershgor, “A Microsoft Employee Literally Wrote Washington’s Facial Recognition Law,” *OneZero*, Medium, April 3, 2020, <https://onezero.medium.com/a-microsoft-employee-literally-wrote-washingtons-facial-recognition-legislation-aab950396927>; and see Lee, “We Need a Face Surveillance Moratorium.”

87 See Spivack and Garvie, “A Taxonomy of Legislative Approaches”; see also Rashida Richardson, ed., “Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force,” AI Now Institute, December 2019, <https://ainowinstitute.org/ads-shadowreport-2019.html>.

88 Section 10, Washington Senate Bill 6280, <http://lawfilesexternal.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729>

What regulatory tools can be used to create public transparency around the development, purchase, and use of biometric recognition tools? ¹

Transparency around the development, purchase, and use of biometric recognition tools ² remains a key barrier to creating public awareness and enforcing existing regulation. Recent advocacy demands include mandatory impact assessments, public notice comment periods, and publicly accessible registries of vendors and uses.

Enforcing existing regulations has been a challenge in part because the development, purchase, and use of biometric tools is often shrouded in secrecy, driven by private firms that have no duty to reveal such “proprietary information.” Once these tools are built, the purchase and subsequent implementation by government, particularly law enforcement agencies, proceeds in ways that are often deliberately hidden from the public. Yet as scrutiny of Clearview AI and subsequent investigations have made clear, there are hundreds of globally distributed vendors selling biometric recognition technology without people’s knowledge or explicit consent. It was only when the Clearview AI story broke that lawsuits were filed under Illinois BIPA, prompting quick action from the company that had violated informed consent requirements when scraping millions of face images off the web.⁸⁹ ³

In recent years, privacy advocates have demanded regulatory tools that ensure transparency as early in the process as possible. Many of these policies target government use to ensure that there is public notice and consultation before these tools are acquired and implemented. For example, in June 2020, after years of civil society advocacy, and in the context of sustained protest against anti-Black police brutality, New York City passed The POST Act, a law that would require the New York Police Department (NYPD) to issue a surveillance impact and use policy about any surveillance technology in use (including biometric recognition tech).⁹⁰ This assessment would include information about capabilities, processes and guidelines, and any safeguards and security measures in place. In the EU, advocacy organizations like Access Now and Algorithm Watch have called for a mandatory disclosure scheme for all AI systems used in the public sector, in conjunction with a mandatory human rights or algorithmic impact assessment.⁹¹ ⁴

Advocates have also demanded that regulation should ensure that external researchers and auditors have access to algorithmic systems in order to understand their workings, as well as the design choices and incentives that informed their development and commercialization, and to engage the public and impacted communities in the process. Meaningful access includes making software toolchains and APIs open to auditing by third parties. ⁵

⁸⁹ Even these faced the barrier of establishing legal standing because it was difficult to confirm that an Illinois resident was in fact part of Clearview’s dataset due to the lack of publicly available information. See *ACLU v. Clearview AI*, <https://www.aclu.org/cases/aclu-v-clearview-ai>.

⁹⁰ The surveillance impact and use policy would first be released in draft form for review by the public. See STOP Spying, POST Act, signed July 7, 2020, <https://www.stopspying.org/post-act>.

⁹¹ Access Now, “Access Now’s Submission to the Consultation on the ‘White Paper on Artificial Intelligence—a European Approach to Excellence and Trust,’” May 2020, https://www.accessnow.org/cms/assets/uploads/2020/05/EU-white-paper-consultation_AccessNow_May2020.pdf.

While advocates continue to push for more transparency, some laws have already enacted certain checks and balances. The GDPR currently has provisions for data-protection impact assessments (DPIA) and “privacy by design” assessments that kick in when there is any “large-scale” processing of biometric data and also in cases of surveillance in publicly accessible spaces. In theory, these offer a robust assessment of the rights implications of the use of these systems, including fundamental questions about necessity and proportionality. However, as Els Kindt notes in her chapter, DPIAs have been challenging to implement in practice, with wide variations across different member countries of the EU. Moreover, the predominant focus on data-protection concerns can leave out inquiries about accuracy or discriminatory impact. Recent proposals around algorithmic impact assessments (AIAs) are structured to include this broader range of concerns and ensure the participation of directly impacted communities in the risk-identification process.⁹²

While transparency and accountability measures have gained momentum, procurement contracts with third-party vendors can inhibit the government’s ability to comply.⁹³ Government procurement of biometric and other forms of AI systems is often confidential due to trade secrecy or other intellectual property claims. When challenged, governments have denied any knowledge or ability to explain and remedy the problems created by these systems. Recent advocacy by civil society organizations and certain city governments in Europe focuses on including standard contractual clauses in these contracts that include waivers to trade secrecy, non-disclosure agreements, or other confidentiality clauses, as well as terms that ensure the process of procurement involves open bidding and public notice.⁹⁴

What role can community-led advocacy play in shaping the priorities and impact of regulation?

Community advocacy to regulate biometrics is growing, playing a crucial role in surfacing evidence of harm, and shaping the rights and protections that policy interventions eventually offer.

Advocacy and mobilization against the use of biometric systems have taken many forms. While traditional digital rights or privacy groups remain active, over the past few years, directly impacted communities have also organized to push back against these systems based on their lived experiences of harm.

92 See AI Now’s detailed AIA framework that public agencies can draw from when implementing AIAs: Dillon Reisman et al., “Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability,” AI Now Institute, April 2018, <https://ainowinstitute.org/aiareport2018.pdf>. The Canadian government’s Algorithmic Impact Assessment tool is also a useful template for regulatory agencies; see Government of Canada, AIA, 2019, <https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/automated-decision-automatise/en/algorithmic-impact-assessment.html>. ICO’s draft auditing framework for AI systems also has helpful guidance on how to document risks, manage inevitable trade-offs, and increase reflexivity at every stage of ADS procurement or development.

93 See *Houston Federation of Teachers v. Houston Independent School District* and *Ark. Dep’t of Human Servs. v. Ledgerwood* cases in Richardson, Schultz, and Southerland, “Litigating Algorithms 2019 US Report.”

94 AI Now Institute, City of Amsterdam, City of Helsinki, Mozilla, and Nesta, “Using Procurement Instruments to Ensure Trustworthy AI,” June 15, 2020, <https://foundation.mozilla.org/en/blog/using-procurement-instruments-ensure-trustworthy-ai/>.

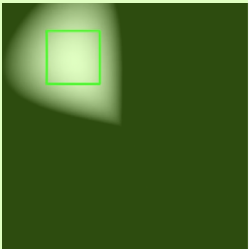
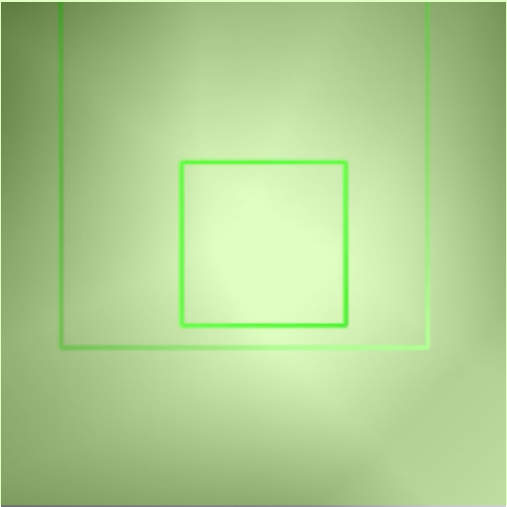
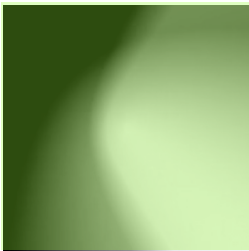
In India, a coalition of privacy groups and grassroots welfare activists formed to publicly protest and legally challenge the Aadhaar biometric ID project.⁹⁵ Against the broad claims of efficiency by the government, the coalition surfaced specific examples of exclusion due to the technical and bureaucratic failures of the system. In their chapter, Stefanie Coyle and Rashida Richardson recount the community-driven advocacy in Lockport, New York, where a group of parents organized against the school district's decision to purchase and deploy facial recognition in schools. Eventually, Coyle and Richardson note, "[p]arents shifted the discourse from debating whether the biometric surveillance system was necessary to focus on the real harms posed to students if the school district decided to move forward." As a result of that advocacy, the New York State Senate introduced a moratorium bill that "mirrors the concerns raised by residents in the community and advocates across the state and country."

Large-scale biometric projects are often promoted in terms of lofty claims about security, accuracy, and efficiency. Community advocacy, particularly on the part of those directly impacted by these systems, has been critical in surfacing key questions like: Efficiency for whom? (In) security for whom? Those required to live under biometric surveillance possess an expertise that cannot be gained by examining these systems at a technical or policy level. There is no way to guarantee the just use of these technologies without centering the experiences of those affected by their use. Recent attempts demonstrate how community interventions can be structured, for example, the "Citizen Biometric Councils" run by the Ada Lovelace Institute in the UK,⁹⁶ and the New York City ADS Task Force "Shadow Report" prepared by a civil society coalition with detailed recommendations to ensure community engagement is meaningful and equitable.⁹⁷ Ultimately, this underscores the importance of community deliberation to the processes that decide whether these systems are used, but also to the kinds of rights and protections that policy interventions eventually offer.

95 See Rethink Aadhaar, <https://rethinkaadhaar.in/>.





96 See Ada Lovelace Institute, "Citizen's Biometric Council" <https://www.adalovelaceinstitute.org/our-work/identities-liberties/citizens-biometrics-council/>

97 Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force", AI Now Institute, 2019, <https://ainowinstitute.org/ads-shadowreport-2019.html>.



TIMELINE OF LEGAL DEVELOPMENTS¹

This timeline tracks the key legal and regulatory developments analyzed in this compendium. The specific chapters where they are discussed are noted below.²

October 2008 ³  4 United States Illinois Biometric Information Privacy Act (BIPA) enacted (See Chapter 8) ⁵	April 2018 ²⁶  27 European Union General Data Protection Regulation (provisions on biometric data) enacted (See Chapter 4) ²⁸ Data Protection Law Enforcement Directive enacted (See Chapter 4)
March 2016 ⁶  8 India ⁷ Aadhaar Act enacted (See Chapter 3) ⁹	September 2018 ²⁹  30 India ³¹ Indian Supreme Court restricts private use of Aadhaar Biometric ID system (See Chapter 3)








2008







2016

2017









2018

2019

April 2019 ¹¹  12 Jamaica ¹³ Jamaican Supreme Court rules biometric ID system unconstitutional (See Chapter 1)	August 2019 ³²  33 International Committee of Red Cross ³⁴ ICRC assembly adopts Biometrics Policy (See Chapter 5)
May 2019 ¹⁴  15 United States ¹⁶ San Francisco ban on government use of facial recognition technology passed (See Chapter 7)	September 2019 ³⁵  36 United States ³⁷ California Body Camera Accountability Act (A.B 1215) (moratorium on existing use of face recognition on body-worn cameras till 2023) passed (See Chapter 7)
June 2019 ¹⁷  18 United States ¹⁹ Somerville, MA ban on government use of facial recognition technology (See Chapter 7)	 38 United Kingdom ³⁹ UK High Court finds Live Facial Recognition permissible, rules out need for new authorizing legislation (See Chapter 6)
July 2019 ²⁰  22 United States ²¹ Oakland, CA ban on government use of facial recognition technology (See Chapter 7)	 40 United States ⁴¹ Justice in Forensic Algorithms Act of 2019 (HR 4368) introduced (See Chapter 1)
 Australia ²³ Identity Service Matching Bill introduced (See Chapter 2)	
 Kenya ²⁴ Huduma Bill (legal authorization for NMIMS project) introduced (See Chapter 1) ²⁵	

October 2019 ¹		November 2019 ¹⁰	
	2 United States ³ No Biometric Barriers to Housing Act (S 2689) introduced (See Chapter 1)		11 United States ¹² The Facial Recognition Technology Warrant Act of 2019 (S 2878) introduced (See Chapter 1)
	Australia ⁴ Identity Service Matching Bill rejected by Australian Parliament (See Chapter 2)	December 2019 ¹³	
	United States ⁵ Berkeley, CA ban on government use of facial recognition technology passed (See Chapter 7) ⁶		14 United States ¹⁵ Northampton, MA ban on government use of facial recognition technology passed (See Chapter 7)
	7 Argentina ⁸ Constitutional challenge to Buenos Aires Live Facial Recognition project (See Chapter 1) ⁹	United States ¹⁶ Alameda, CA ban on government use of facial recognition technology passed (See Chapter 7) ¹⁷	
		United States ¹⁸ Brookline, MA ban on government use of facial recognition technology passed (See Chapter 7) ¹⁹	

2019		2020

January 2020 ²¹		June 2020 ³⁴	
	22 United States ²³ Cambridge, MA ban on police use of facial recognition technology passed (See Chapter 7)		35 United States ³⁶ Facial Recognition & Biometric Technologies Moratorium Bill S 4084 introduced (See Chapter 7)
	24 Kenya ²⁵ Kenyan High Court suspends NMIMS biometric ID project (See Chapter 1)	United States ³⁷ New York Public Oversight of Surveillance Technology (POST) Act (Int 0487-2018) passed (See Chapter 1)	
	United States ²⁶ California Consumer Privacy Act (provisions on biometric data) enacted (See Chapter 1) ²⁷	July 2020 ³⁸	
February 2020 ²⁸			39 United States ⁴⁰ New York Senate Bill S5140B (regulating biometric technologies in school) passed (See Chapter 9) ⁴¹
	29 United States ³⁰ Springfield, MA moratorium on government use of facial recognition technology passed (See Chapter 7)	August 2020 ⁴²	
March 2020 ³¹			43 United States ⁴⁴ National Biometric Privacy Act (S ____) introduced (See Chapter 1)
	32 United States ³³ Washington SB 6280 (regulates government use of facial recognition technology) passed (See Chapter 7)		

Australian Identity-Matching Services Bill¹

Jake Goldenfein (Melbourne Law School)²
Monique Mann (Deakin University)

Since 2017, the Australian federal government has pushed for political and legal changes to make facial recognition technology more widely available to civil and policing agencies. These efforts, part of a long-term and continuing expansion of surveillance powers by the Australian federal government, have culminated in a new biometric identity-information system. Federal authorities have argued that facial recognition technology is useful for law enforcement and preventing identity fraud, but to achieve those benefits, they have combined civil and criminal, as well as state and federal, identity systems into a powerful intelligence apparatus controlled by a single government department: the Australian Department of Home Affairs.³

Home Affairs was created in 2017 through a merger of the Department of Immigration and Border Protection and the Australian Border Protection Service. As a result of the merger, Home Affairs assumed multiple policing and intelligence competencies from the Attorney General's Department (AGD), including those related to national security, immigration, organized crime, cybersecurity, and public safety policing. Home Affairs also took over control and operation of the national identity-matching services, which included the one-to-one facial recognition verification system known as the "Face Verification Service" (FVS).⁴

¹ One-to-one verification means that an image is submitted along with a stated identity, and the system responds with a "yes" or a "no." The purpose is to prevent identity fraud by ensuring an individual presenting to an agency is who they claim to be.

The Australian government has been developing the institutional, technical, and legal architecture for facial recognition capabilities for several years,² culminating in the 2019 federal Identity-Matching Services Bill.³ The original bill was rejected, however, for a lack of privacy protection and oversight, and is presently being redrafted. The new bill will likely increase parliamentary oversight of the system and the amount of necessary reporting, but will not challenge the fundamental institutional changes that are already underway, such as the aggregation of civil and criminal systems, or increased control of state-level civic data within a federal intelligence system.

Although governments have always had the function of identifying their citizens,⁴ they have not always linked those identities to intelligence dossiers or made them available to law enforcement agencies. Indeed, the intermingling of civil and criminal identity systems has been the concern of human rights jurisprudence for some time.⁵ Biometrics are of particular concern to the linkage of criminal and civil systems, and surveillance more generally, because they act as a conduit between an individual's physical presence and digital databases, thus amplifying surveillance capacities. By advancing a centralized identity matching system, Australia is pushing beyond the limits of legitimate state function.

BIOMETRICS DEVELOPMENT IN AUSTRALIA³

Australia has collected biometric information, including images for facial recognition, since at least 2007. This began with border-protection agencies collecting information from noncitizens, such as people caught fishing illegally in Australian waters, and eventually from visa applicants. It has progressively expanded to include information collected from Australian citizens, both at the border and through civic licensing agencies.⁶ States have also used biometric systems for matching against their police information holdings (i.e., mug shot databases) since at least 2009.⁷

The 2007 Intergovernmental Agreement to a National Identity Security Strategy⁸ proposed the development of a national biometric interoperability framework,⁹ which was launched in 2012.¹⁰ Plans for a further national facial biometric matching "Capability" to enable cross-jurisdictional sharing of identity information, the precursor to the identity matching system operated by Home Affairs, were announced in 2014.¹¹

2 See, e.g., Australian Government, Department of Home Affairs, "Agreement to a National Identity Security Strategy," April 2007, <https://www.homeaffairs.gov.au/criminal-justice/files/inter-gov-agreement-national-identity-security-strategy.pdf>.

3 Identity-Matching Services Bill 2019 (Cth). The note (Cth) indicates that this is a commonwealth or federal bill. The Identity-Matching Services Bill was first introduced in February 2018, but did not progress through parliament and lapsed in April 2019. It was reintroduced in July 2019.

4 See, e.g., Markus Dirk Dubber, *The Police Power: Patriarchy and the Foundations of American Government* (New York: Columbia University Press, 2005).

5 See, e.g., Jake Goldenfein, *Monitoring Laws: Profiling and Identity in the World State* (Cambridge: Cambridge University Press, 2019).

6 Dean Wilson, "Australian Biometrics and Global Surveillance," *International Criminal Justice Review* 17, no. 3 (September 2007): 207–219.

7 Parliament of Australia, "CrimTrac Overview 2009" (direct download, PDF), <https://www.aph.gov.au/DocumentStore.ashx?id=dd60984f-33e2-4836-85a4-690052ca7914>.

8 Australian Government, Department of Home Affairs, "An Agreement to a National Identity Security Strategy," April 2007, <https://www.homeaffairs.gov.au/criminal-justice/files/inter-gov-agreement-national-identity-security-strategy.pdf>.

9 Australian Government, Department of Home Affairs, "A National Biometric Interoperability Framework for Government in Australia," n.d., <https://www.homeaffairs.gov.au/criminal-justice/files/national-biometric-interoperability-framework-for-government-in-australia.pdf>.

10 Attorney-General's Department, *National Identity Security Strategy 2012*, Canberra, 2013.

11 Law, Crime and Community Safety Council, *Communique*, COAG Meeting, Canberra, October 3, 2014, <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/3523779%22>.

The one-to-one face verification system (FVS) that Home Affairs took over from the Attorney-General's Department (AGD) began operating in 2016, but only included passport images held by the federal Department of Foreign Affairs and Trade (DFAT).¹² Given the uptake of driver's licenses in the general population and the ambition for a national system, the policy goal has long been to integrate state-controlled driver's license images into a general database for policing and intelligence.¹³ Efforts by federal entities to access driver's license images have been, however, frustrated by state privacy laws, which prohibit providing federal agencies direct access to their databases.¹⁴ The result has been limited and complex arrangements for cross-jurisdictional information sharing. This began to change, however, with the 2017 Intergovernmental Agreement on Identity Matching Services (IGA)¹⁵—the precursor to the Identity-Matching Services Bill—and the corresponding formation of the Department of Home Affairs, with its very broad federal policing and intelligence remit.

CENTRALIZATION OF IDENTITY DATABASES²

In 2017, the Australian states agreed multilaterally to enable federal access to their identity data under the auspices of the IGA. Some states made explicit the value they saw in the system, with the Queensland Minister for Police noting the value that one-to-many facial recognition would contribute to enhanced security at the Commonwealth Games.¹⁶ Other states were more reluctant, raising the alarm about possible contravention of state-level human rights protections, and suggesting that there were inadequate protections for civil liberties.¹⁷

Nonetheless, the IGA established the framework for a data-sharing regime, gave immunity from state-level privacy laws, and introduced new identity-matching services, including a one-to-many facial identification service (FIS) to complement the FVS. Such systems are the primary facial recognition tool used in policing in Australia. The system allows for law enforcement, national security, and related entities at state and federal level to run queries through the technical infrastructure of a host agency: originally the AGD, and then the Department of Home Affairs. Importantly, while the IGA introduced a technical architecture for information sharing, it left control over identity databases with the states.¹⁸

- 12 See Allie Coyne, "Australia's New Facial Verification System Goes Live," *IT News*, November 16, 2016, <https://www.itnews.com.au/news/australias-new-facial-verification-system-goes-live-441484>. That federal system was populated by passport photos, which in 2010–2011 covered approximately 48 percent of the Australian population (Department of Foreign Affairs and Trade (Cth), "Program 2.2: Passport Services," *Annual Report 2010–2011*, <https://nla.gov.au/nla.obj-990174440/view?partId=nla.obj-994334219#page/n161/mode/1up>) and presently covers about 57.9 percent of the population (<https://www.passports.gov.au/2019-passport-facts>).
- 13 Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Strengthening Oversight," *UNSW Law Journal* 40, no. 1 (2017): 121–145.
- 14 See, e.g., the Parliament of the Commonwealth of Australia, "Identity Matching Services Bill 2019, Explanatory Memorandum," describing Clause 19 of the Bill. An exception is the NSW Roads and Maritime Services, which provides access to the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) for the purposes of investigating terrorism offenses.
- 15 Council of Australian Governments, "Intergovernmental Agreement on Identity Matching Services," October 5, 2017, <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>.
- 16 Mark Ryan, "Queensland Leads Nation to Strengthen Security Measures," Queensland Government, The Queensland Cabinet and Ministerial Directory, March 7, 2018, <http://statements.qld.gov.au/Statement/2018/3/7/queensland-leads-nation-to-strengthen-security-measures>.
- 17 See, e.g., Adam Cary, "Biometrically Opposed: Victoria Queries Peter Dutton over Facial Recognition Scheme," *Sydney Morning Herald*, May 2, 2018, <https://www.smh.com.au/politics/federal/biometrically-opposed-victoria-queries-peter-dutton-over-facial-recognition-scheme-20180502-p4zcv5.html>.
- 18 Note that the IGA architecture replicates, and was perhaps inspired by, the FBI's Next Generation Identity system, launched in 2014. See FBI, Next Generation Identification (NGI), <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

A few months later, the government introduced the Identity-Matching Services Bill, which ostensibly legislated for the IGA. In reality, however, the bill went significantly further, shifting the system from one that facilitated information sharing into one that enabled the aggregation and centralization of identity information in the Department of Home Affairs.

This increased centralization is in no way integral to satisfying the objectives of the system, at least as publicly stated. The bill's explanatory memorandum, for instance, outlined the primary goal as preventing fraud and identity theft (described as an enabler of organized crime and terrorism), but not to build an intelligence apparatus.¹⁹ Despite the limited technical capacity necessary to achieve that stated objective, the system specified in the bill would fold state-level transport authorities' data and images into the data-intensive apparatuses of federal security and intelligence agencies.

The centralizing dimensions of the system architecture become apparent when looking closely at the differences between the IGA and the bill. Beyond addressing identity fraud, we suggest these changes reveal the true underlying political rationalities and motivations for establishing this national facial recognition system as a radical shift in identity data governance arrangements.

LEGAL CONCENTRATION OF POWER

The Identity-Matching Services Bill sought to establish Home Affairs as the "hub" through which government identity-verification and law enforcement suspect-identification requests are processed, establishing Home Affairs as the central point of information processing across the public sector and for law enforcement agencies. But there were meaningful departures from the system described in the bill and the 2017 IGA.

The IGA outlined two technical architectures: 1) The National Driver License Facial Recognition Solution (FRS), a biometric identity image database; and 2) the "interoperability hub," a communications system for processing and routing data access requests from agencies around Australia.

In the IGA, the FRS was described as a federated database system, in which state-level data would be partitioned, and state agencies could control the conditions of access. Databases would be linked through Home Affairs, which would operate the facial recognition technology that performs identity matching. The FRS was described as retaining only biometric identity templates and no other identity or personal data. The IGA stipulated that the host agency (initially the AGD, but subsequently Home Affairs) could not view, modify, or update information in partitioned federated databases containing state-level information. However, the bill only prescribed that Home Affairs could not modify or update that data; in other words, it could still view it.²⁰ In fact,

¹⁹ The Australian Government IDMatch home page, for example, promotes "Identity Matching Services that help verify and protect your identity" (<https://www.idmatch.gov.au>). See also the Parliament of the Commonwealth of Australia, "Identity Matching Services Bill 2019, Explanatory Memorandum," https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6387_ems_f8e7bb62-e2bd-420b-8597-8881422b4b8f/upload.pdf/713695.pdf;fileType=application%2Fpdf.

²⁰ Sup. 11. See IGA clause 6.16.

the legislation clarified that Home Affairs *could* collect, effectively without limit, information flowing through the systems for satisfaction of its “community safety” purposes, which include law enforcement, national security, community safety, protective security, and road safety, along with identity verification. The bill effectively vested control over the databases of driver’s license images squarely within Home Affairs, and enabled unrestrained collection of information. ¹

With respect to the “interoperability hub,” the IGA described it as a “router” through which agencies around the country could request and transmit information to one another. That is, it could be used for “relaying electronic communications between bodies and persons for the purposes of requesting and providing identity-matching services.” Rather than simply routing information from place to place, however, the bill enabled Home Affairs to collect data flowing through the hub whenever an agency used an identification, verification, or information sharing service, both for the sake of operating that database,²¹ as well as for its identity and community protection activities.²² The bill thus enhanced the legal capacity of Home Affairs from an infrastructure provider into a data aggregator. ²

Other important elements of the bill gave greater power than envisaged to the Department of Home Affairs. For instance, the bill enabled the Minister for Home Affairs to expand the powers under the regime without parliamentary oversight. Furthermore, the identity information that could be collected through those systems was far broader than anticipated by the IGA,²³ including information held by agencies that is about or associated with the identity document. ³

It is difficult to identify a single rationale that may have motivated the changes between the IGA and the Identity-Matching Services Bill. New technological affordances associated with facial recognition may have animated interest in developing a comprehensive national system, especially considering international trends. The institutional culture and political power of the Department of Home Affairs may also have made centralization and the use of civil documents in intelligence investigation more feasible. Indeed, its participation in forms of intelligence work and political policing connects it to a policing tradition that has always involved information aggregation, not necessarily in line with traditional liberal political limits.²⁴ That expansion of political and technological power is also consistent with Home Affairs’ broad portfolio. ⁴

Australia lacks enforceable human rights protections at the federal level (though some states have their own independent human rights protections), which raises a number of issues and concerns with the centralization of data and surveillance capabilities within federal agencies. Under the Australian Constitution,²⁵ crime control and criminal justice are a competency of the states, not the federal government. Policing agencies are historically restricted to identity matching against data in local policing information systems (such as mug shots), which ⁵

²¹ Sup. 3. See § 17 (2).

²² Sup. 3. See § 17(2)(b); note that the purposes for which Home Affairs can collect data flowing through the interoperability hub is not clear in the legislation because it is split over two provisions. However, it has been interpreted to mean collection is permitted for the broader range of purposes (Bills Digest).

²³ In the Bill, § 5; in the IGA, clause 3.1.

²⁴ See, e.g., Bernard Porter, *The Origins of the Vigilante State: The London Metropolitan Police Special Branch before the First World War* (London: Weidenfeld and Nicolson, 1987).

²⁵ *Commonwealth of Australia Constitution Act 1900* (Cth).

have comprehensive rules and limits on retention.²⁶ As Home Affairs moves to aggregate and centralize biometric data, it is violating privacy norms by way of “scope creep,” i.e., generating data for one government purpose (e.g., licensing drivers), and using it for another (e.g., policing or other punitive applications).¹

PJCIS REJECTS THE BILL²

Ultimately, the Identity-Matching Services Bill did not pass parliamentary scrutiny and was rejected by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). But the specific issues that led to its rejection are unlikely to halt the system’s development. In fact, the rejection can be interpreted as an endorsement of the general system and the resultant centralization, subject to privacy and accountability “tweaking.”³

When the bill reached the PJCIS, it was rejected largely due to concerns that it would grant too much executive authority to the Department of Home Affairs, meaning that the Minister for Home Affairs could change rules without legislative oversight.²⁷ The PJCIS also echoed the fears of privacy advocates around the possibility of a real-time, facial recognition-powered CCTV mass surveillance system which could end anonymity in public and stifle political action like protesting. The report also noted accountability issues like the absence of judicial warrant requirements, and the lack of a dedicated biometric oversight body (both of which exist in the United Kingdom).⁴

On a broader level, the PJCIS expressed anxieties around the system not being proportionate to the issues it purported to solve, or sufficiently privacy-protective. But those concerns were connected to possible problematic “uses” of the system, not the broader structural issues of data centralization or the aggregation of civil and criminal identity databases. Instead, there was general approval that this type of data sharing would occur subject to a binding legislative framework rather than through creative interpretations of law enforcement and security exemptions to privacy laws.²⁸⁵

26 Jake Goldenfein, “Police Photography and Privacy: Identity, Stigma, and Reasonable Expectation,” *University of New South Wales Law Journal* 36, no. 1 (2013): 256–279.

27 See Parliament of Australia, “Review of Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-Matching Services) Bill 2019,” n.d., https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019.

28 See the “Parliamentary Joint Committee on Intelligence and Security” (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security), the “Advisory Report on the Identity-Matching Services Bill 2019 and the Australian Passport Amendment (Identity-Matching Services) Bill 2019” (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report), and “A Workable Identity-Matching Regime” (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report/section?id=committees%2Freportjnt%2F024343%2F27805). Specifically, the PJCIS argued that the Identity-Matching Bill is designed to “permit all levels of government and the private sector unprecedented access to Australian citizens’ private biometric information in the form of a facial image” and that “given the significance of these measures, the Committee considers it preferable that privacy oversight and safeguards are established and set out in this enabling legislation rather than only being provided in supplementary agreements or arrangements.”

The PJCIS accordingly recommended redrafting the bill to make its function and purpose clearer to the ordinary reader, reduce Ministerial rule-making power, fund a biometric oversight commission, and require more comprehensive reporting.²⁹ The PJCIS did not, however, completely reject the bill, the use of facial recognition technology, or the new data governance arrangements that would power the system.

FUTILITY OF AUSTRALIAN REGULATORY OVERSIGHT

The Identity-Matching Services Bill is presently being redrafted, with the new text yet to be released. Nonetheless, the states continue to upload identity images to the system in anticipation of the law passing and the system developing along similar lines. One reason political review has failed to meaningfully challenge the general structure of the identity matching and facial recognition system is that the debate, especially as expressed in the PJCIS report, has taken up a “privacy versus security” framing. International human rights law requires that state surveillance be “reasonable” and “proportionate,” and this language clearly influenced the PCJIS.

Under a human rights framework, to legitimately limit fundamental freedoms like privacy, a surveillance intervention must be directly related to, and the least restrictive measure for, the “necessary” purpose pursued. A true proportionality analysis might question whether such dramatic data governance rearrangements are necessary to address the stated purpose of identity fraud. In reality, however, this framing is operationalized in ways that enable continuing expansion of surveillance systems, especially in nations like Australia, where it is not backed up by actionable protections.

When privacy is pitched against security, the benefits of centralization and surveillance technology to purposes like identity fraud are taken as given, and the question becomes: Which civil liberties are we willing to curtail or limit in exchange? Blanket data sharing for policing and intelligence agencies is thus readily accepted and normalized as a necessary response to crime and insecurity, subject to privacy *balancing* intended to curtail its most abusive and authoritarian dimensions.³⁰ That framing fails to address the reality that the system fundamentally eliminates the need for the largest policing and intelligence apparatus in the country to justify its access to personal data that was previously distributed to the states. This goes beyond agencies using biometrics for their democratically constituted civic purposes (e.g., driver’s licenses), and beyond the stated intention of the bill (e.g., detecting identity fraud). By pushing this bill forward, Home Affairs is promoting facial recognition technology as a necessary solution to identity crime, while sidelining concerns around the institutional and data governance rearrangements that it claims are necessary for its introduction.

29 It should be noted that there are oversight bodies responsible for Commonwealth law enforcement agencies under the Law Enforcement Integrity Commissioner Act 2006 (Cth) that established the Commonwealth Integrity Commissioner and the Australian Commission for Law Enforcement Integrity, which has jurisdiction over all Commonwealth law enforcement agencies (including those responsible for the facial biometrics matching system).

30 See, for example, Monique Mann et al., “The limits of (Digital) Constitutionalism? Exploring the Privacy-Security (Im)balance in Australia,” *International Communication Gazette* 80, no. 4 (2018), 369–384.

From this position, it becomes impossible to challenge the construction of the surveillance system, or to fight the technical or institutional architecture, in any meaningful way. The institutional momentum also makes resisting significant data governance rearrangements difficult. One recent positive development, however, has been the Australian Human Rights Commissioner calling for a moratorium on the use of facial recognition technology as part of the Technology and Human Rights Project, which mirrors some international trends.³¹ However, it is uncertain what impact this will have on the design, development, and eventual deployment of facial recognition technology in Australia, especially considering the extent to which the infrastructure is already in place.

1

Finally, technologies like Clearview AI, which has aggregated billions of identified images from the public web, complicate how to parse these developments.³² Private providers, not constrained in the same way, can undermine relevant privacy protections or political processes by secretly selling surveillance services to government, while using their own privately operated infrastructure. When governments procure those services, they bypass whatever regulatory or financial obstacles might have prevented or limited those developments by the state itself. To that end, it is at least admirable that the Australian identity matching regime will be implemented in law, subject to democratic process and parliamentary oversight. Nonetheless, even when that is the case, the purposes expressed to justify new facial recognition *implementations* for the sake of those democratic processes appear not to tell the full story. It remains imperative to identify and address the institutional realignments and data governance reconfigurations connected to technologies like facial recognition and not be distracted by any single new surveillance capacity.

2

31 Australian Human Rights Commission, "Human Rights and Technology Discussion Paper," December 2019, <https://www.humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019>.

32 "Australian police agencies initially denied they were using the service. The denial held until a list of Clearview AI's customers was stolen and disseminated, revealing users from the Australian Federal Police as well as the state police in Queensland, Victoria and South Australia." See Jake Goldenfein, "Australian Police Are Using the Clearview AI Facial Recognition Technology with No Accountability," *The Conversation*, March 4, 2020, <https://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667>.

The Economy (and Regulatory Practice)¹ That Biometrics Inspires: A Study of the Aadhaar Project

Nayantara Ranganathan (lawyer and independent researcher, India)²

The Government of India launched the Aadhaar biometric identity project in 2009 with the aim of providing identification for all residents.¹ The project called for a centralized database that would store biometric information (fingerprints, iris scans, and photographs) for every individual resident in India, indexed alongside their demographic information and a unique twelve-digit “Aadhaar” number. India’s now-dissolved Planning Commission formed the Unique Identification Authority of India (UIDAI) to plan the project, as well as implement and perform regulatory functions.² The scale and ambitions of the project are matched only by the long and rich history of resistance to it. Economists, technologists, people’s movements, and concerned citizens have questioned the amplified surveillance dangers, indignities from exclusion due to failures in biometric identification systems, and lack of institutional accountability.³ The project proceeded without any legal framework to govern it for seven years after its inception (government use of data in India is still not governed by any dedicated law).

1 Government of India, Planning Commission, “Notification No. A-43011/02/2009-Admn.I,” January 28, 2009, https://uidai.gov.in/images/notification_28_jan_2009.pdf (last accessed on July 15, 2020). UIDAI was set up under the chairmanship of one of the foremost industry leaders of the Indian IT sector, Nandan Nilekani.

2 Ibid.

3 For some critiques by technologists, see, for example, Rethink Aadhaar, <https://rethinkaadhaar.in/>; and the Medium site *Kaarana*, <https://medium.com/karana>. For a compilation of dissenting notes by various authors, see Reetika Khera, ed., *Dissent on Aadhaar: Big Data Meets Big Brother* (Hyderabad: Orient Blackswan, 2019).

Responding to the glaring lack of accountability raised by public advocacy and litigation, the Indian government passed the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act⁴ in 2016, with negligible public or parliamentary debate.⁵ While the law provided some procedural safeguards around biometric data security and consent, the law should be understood as a part of a broader institutional and economic project to instrumentalize biometric information in the service of the data economy. This essay explores the continuing legal and regulatory complicity in constructing data as a resource for value extraction, and how regulatory practice mimics the logics and cultures of the technologies it seeks to regulate.

MAKING DATA MARKET-READY²

The law goes to great lengths to sustain the idea of biometric data as signifying truth, supporting and maintaining an infrastructure that is foundational for the data economy.

*The Truth about Biometrics*⁴

Early planning documents of the Aadhaar project refer to biometrics as a fundamental identity, while older forms of identification based on demographic information are considered “surrogates of identity.”⁶ Yet biometric information is also a class of media, offering representations of bodily attributes captured at a particular moment in time under specific material conditions, and of no greater epistemic caliber. However, when coupled with the moral timbre of truth, biometric information can perform the important function of instituting people as data points within databases. This allows datafication of flows like cash exchanges or road traffic to be easily mapped onto signifiers of “real” people within databases, making these newly captured and latent dataflows more meaningful and profitable.

In the Aadhaar project, high-resolution photographs of people’s irises and fingerprints were collected at the time of enrollment into the database, along with standard photographs of faces.⁷ An equivalence between media artifacts captured about a person and their true identity might

4 Hereinafter called the Aadhaar Act, or simply Aadhaar. For the text of the act, see the Ministry of Law and Justice, “The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,” 2016, March 26, 2016, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

5 See Ujjwala Uppaluri, “The Aadhaar Programme Violates Democratic Process and Constitutional Rights,” *Caravan*, April 4, 2017, <https://caravanmagazine.in/vantage/aadhaar-violates-democratic-process-constitutional-rights>. See also Software Freedom Law Center (SFLC), “How Parliament Debated the Aadhaar Bill, 2016,” March 19, 2016, <https://sflc.in/how-parliament-debated-aadhaar-bill-2016>.

6 UIDAI, “Role of Biometric Technology in Aadhaar Enrollment,” January 21, 2012, http://www.dematerialisedid.com/PDFs/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf. See also UIDAI, “Basic Knowledge of UIDAI and Aadhaar, Module 1,” March 16, 2015, https://uidai.gov.in/images/training/module_1_basic_knowledge_of_uidai_and_aadhaar_16032015.pdf.

7 UIDAI, “Aadhaar Enrollment Process,” <https://uidai.gov.in/contact-support/have-any-question/296-faqs/enrolment-update/aadhaar-enrolment-process.html>.

be common in popular parlance, but with Aadhaar, such an equivalence was crystallized in law.⁸ Yet this equivalence is neither natural nor logical. The jump from the material facts of these representational media to their revelatory quality is a tactical one that several actors in the data economy are invested in maintaining. Aadhaar intends to act as both a unique and ubiquitous⁹ signifier, offering itself as part of an “identity layer” that may then be used as a foundation for the datafication of realms like finance, taxation, healthcare, and education.¹⁰

Grooming Uniqueness as Truth²

For practical as well as ethical reasons, the use of biometrics as a stand-in for unassailable truth about people is suspect.¹¹ But law and regulation have worked to prop up this fiction and attach market value to it, through the legally defined processes of “deduplication,” the mandatory updating of biometrics information, and the reputational coupling of demographic and biometrics data.

Deduplication: At the time of enrollment in Aadhaar, all biometrics information is checked against every other entry in the database.¹² Deduplication is often seen as a best practice in biometrics enrollment, but its role in solidifying assumptions about the nature or suitability of biometrics for purposes of identification or authentication is not equally recognized. Deduplication confirms the uniqueness of each entry’s biometric information, within the database and for the *limited purpose* of the database.

Updating biometrics information and technology: While uniqueness is architected through deduplication, fidelity of the media at the time of enrollment to the biological attributes of individuals cannot be sustained for reasons like fingerprints and irises changing over time, as well as several types of fraud.¹³ Rather than questioning the wisdom of using biometric information as a fundamental identity and an authentication key, the law uses minor fixes while still equating biometric information with biological attributes. The law gives UIDAI powers to

8 Erasure of the fact of mediation surfaces in the definition of “biometric information.” Notice that in the definition of “biometric information” in Section 2(g) of the Act, there is a slippage or equivalence between media (e.g., a photograph) and the subject (e.g., a fingerprint). In other words, there is a slippage and equivalence between biological attributes and their representation that is captured in the machines. Section 2(g) states that “biometric information means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.” This erasure is again reiterated in the definition of “core biometric information” in Section 2(j): “core biometric information’ means fingerprint, iris scan, or such other biological attribute of an individual as may be specified by regulation.” A definition not making this erasure might read as follows: “core biometric information’ means fingerprint, iris scan, or such other *representations* of biological attributes of an individual as may be specified by regulation.”

9 Usha Ramanathan, “Aadhaar—From Welfare to Profit,” in *Dissent on Aadhaar: Big Data Meets Big Brother*, ed. Reetika Khera (Hyderabad: Orient Blackswan, 2019), 178.

10 See “Basic Knowledge of UIDAI and Aadhaar, Module 1,” https://uidai.gov.in/images/training/module_1_basic_knowledge_of_uidai_and_aadhaar_16032015.pdf.

11 For a discussion of the issues surrounding use of biometrics as a stand-in for truth about people, e.g., with creating a “self-referential system” that is unconcerned with the realities of aging, machine quality, and fraud, see Nishant Shah, “Identity and Identification: The Individual in the Time of Networked Governance,” *Socio-Legal Review* 11, no. 2 (2015): 22–40, <http://docs.manupatra.in/newsline/articles/Upload/D47CF36C-C409-45BF-8AE6-659D7B6281FB.pdf>; on the harms of treating bodies as data, see Anja Kovacs, “When Our Bodies Become Data, Where Does That Leave Us?,” *Deep Dives*, May 28, 2020, <https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969>.

12 UIDAI, “Features of Aadhaar” <https://uidai.gov.in/my-aadhaar/about-your-aadhaar/features-of-aadhaar.html>.

13 The only kind of fraud that biometrics protects against is the enrollment of the same person more than once.

require Aadhaar holders to update their biometric information from time to time, at their own cost,¹⁴ “to ensure continued accuracy” and not, say, to correct the inevitable deterioration of fidelity of biometric information.¹⁴ The law even anticipates, supports, and relies on ever-better biometrics technologies, bridging any imagined distance between a thing and its representation.¹⁵

Lending truth to demographic data: Biometrics’ reputation of truth, and its resultant market value, are also transposed onto the corresponding demographic information (like name, gender, address) and the unique twelve-digit Aadhaar number generated.¹⁶ However, such demographic data does not benefit from the same heightened data-security protections,¹⁷ is unverified, and is unaudited.

KEEPING DATA MARKET-READY³

Aadhaar has been described as “a government programme run with the energy of a private sector start-up,”¹⁸ and is emblematic of the close cooperation between private actors and UIDAI. As a result of these close ties, regulation of the Aadhaar project enacts itself as cybernetic feedback loops that are constantly adapting to unfavorable changes, optimized toward keeping an infrastructural building block of the data economy alive.

*Aadhaar as a Building Block*⁵

From the outset, the UIDAI envisioned Aadhaar as an identity “platform”: an infrastructure that would provide authentication and verification services, and satisfy a necessary precondition for the data economy to thrive.¹⁹ Indeed, the law emphasizes the importance of Aadhaar as a source of identification for the marginalized, and to enable efficient and targeted welfare delivery.²⁰

14 See Section 6 of the Aadhaar Act (https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf). The Act places the responsibility of such updates with the Aadhaar number holder.

15 The Aadhaar Act anticipates and privileges the proliferation of biometrics technologies by including an expansive definition of biometrics; see Section 2(g) of the Act. Additionally, the Act also reserves the power of UIDAI to promote research and development for advancement in biometrics and related areas; see Section 23(2)(q) of the Act.

16 The Aadhaar number is used for various purposes, including bank verification, despite the low quality of data and its unverified and unaudited nature.

17 On the authentication of the Aadhaar number, see Section 8 of the Aadhaar Act; on the restriction on sharing information, see Section 29; on biometric information deemed to be sensitive personal information, see Section 30. Conversely, where concerns around the Aadhaar project have arisen, they are allayed by a false sense of safety provided for the biometric information, while the associated demographic information fills any gaps created by the withdrawal of biometrics.

18 Viral Shah, “Like Narendra Modi, Nandan Nilekani Too Understands the Transformative Power of Technology,” *India Today*, September 16, 2017, <https://www.indiatoday.in/magazine/news-makers/story/20170925-pm-narendra-modi-nandan-nilekani-aadhaar-ekyc-gst-artificial-intelligence-1044702-2017-09-16>.

19 The Biometrics Standard Committee set up by the UIDAI in its report as far back as December 2009 stated that the UIDAI would “create a platform to first collect identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers.” See UIDAI, “Biometrics Design Standards for UID Applications,” December 2009, <https://archive.org/details/BiometricsStandardsCommitteeReport/mode/2up>. See also Ramanathan, “Aadhaar—From Welfare to Profit,” 177.

20 See Krishnadas Rajagopal, “Centre’s Aadhaar Affidavit in Supreme Court: ‘Welfare of Masses Trumps Privacy of Elite,’” *The Hindu*, June 9, 2017, <https://www.thehindu.com/news/national/centres-aadhaar-affidavit-in-supreme-court-welfare-of-masses-trumps-privacy-of-elite/article18951798.ece>; and see the Preamble of The Aadhaar Act.

However, Aadhaar's market function has been understated; early documents indicate that the project was preoccupied with its role of instituting people as data points within existing and new databases.²¹

At the outset, this authentication infrastructure took the form of application programming interfaces (APIs)²² for use by government agencies and third parties, for verification and authentication of identity information.²³ Such an instrumentalization of the Aadhaar database not only drastically reduced the costs of performing door-to-door verification required of banking and telecom service providers, but also held the promise of entirely new use cases for businesses.²⁴

These APIs are part of "India Stack," a growing set of APIs built by a group of self-styled volunteers called India Software Products Roundtable (iSPIRT), or Product Nation.²⁵ iSPIRT designs and builds these APIs for use by government entities and businesses alike, in the process creating novel opportunities for value extraction from data flows and populating the Aadhaar ecosystem.

Aadhaar Integration with Cooperation of Sectoral Regulatory Institutions

With a strong need for identity verification, the finance sector was the first to fully embrace Aadhaar. With the close cooperation of UIDAI and iSPIRT, institutions within the finance sector²⁶ led efforts to build technology products forming a cashless layer atop the Aadhaar identity layer.

These products allowed banks to use the Aadhaar number to make remittances²⁷ or to authorize Aadhaar-linked bank accounts to transact through biometric authentication,²⁸ and allowed firms to query the Aadhaar database to verify and onboard customers.²⁹ With these Aadhaar integrations into legacy banking services in place, NPCI launched a payments system that introduced interoperability between different payments and settlements systems through the

21 Consider, for example, the orientation of the UIDAI Security Policy and Framework for UIDAI Authentication, which provided mandatory and recommendatory security considerations to Authentication User Agencies (AUA), Authentication Service Agencies (ASA), Devices, etc. This document, speaking directly to security and privacy concerns, which are traditionally welcome as areas of regulation, primarily deals with network security concerns like distributed denial of service (DDOS) attacks that protect the conditions that are critical for the authentication infrastructure to run seamlessly. While no doubt this is required, the policy is entirely unconcerned with simpler and more commonplace risks that have proven to affect individuals to disastrous effect. For example, people who were not used to treating erstwhile ID cards as private information continued to share their Aadhaar numbers and related information with no hesitation, sometimes compromising their economic security. The mandate to guard against security risks that such socially grounded identification cultures bring is not something that any of the regulatory agencies concern themselves with.

22 "An API is a set of definitions and protocols for building and integrating application software...APIs let a product or service communicate with other products and services without having to know how they're implemented." See "What Is an API?" RedHat, <https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces>.

23 Aadhaar Authentication API: returns "yes/no" responses to queries seeking authentication of biometric or demographic data. Aadhaar electronic Know-Your-Customer (eKYC) API: returns demographic information in response to queries.

24 Aman Sharma, "The Private Sector Can Use Aadhaar Authentication Too: UIDAI," *Economic Times*, April 5, 2016, <https://economictimes.indiatimes.com/news/politics-and-nation/private-sector-can-use-aadhaar-authentication-too-uidai/articleshow/51691531.cms>.

25 See iSPIRT, <https://ispirt.in/>.

26 E.g., the National Payments Corporation of India (NPCI); and the central bank and finance regulator, Reserve Bank of India.

27 See Aadhaar Payments Bridge System, a new batch processing system implemented by NPCI.

28 See Aadhaar Enabled Payment System.

29 See Aadhaar-based Biometric Authentication and electronic Know-Your-Customer norms.

introduction of Aadhaar biometric authentication, among others.³⁰ In practical terms, private firms could now build payment-related products and users could easily make payments through their smartphones. As a cohesive suite of technology “platforms,” these products and switches³¹ enabled the creation, capture, and monetization of data flows in finance.³²

UIDAI and its private-sector financial partners planned for the interoperability between Aadhaar and financial tools from the start,³³ and conflicts of interest were notable. People associated with building the cashless layer went on to launch startups that created novel ways of payment-data monetization. Venture capitalists associated with the cashless layer went on to back these very startups.³⁴

Nevertheless, the government and financial sector have argued that this ecosystem is a boon for financial inclusion.³⁵ As a testament to its value, Nandan Nilekani notes that securing a loan has now become as simple as having “a richer digital footprint.”³⁶

However, these narratives recast complex sociopolitical issues like lack of access to banking as individual journeys of competition for artificially scarce resources, to be won by participating and winning in the data economy. These interventions are far from actually addressing issues of financial inclusion.³⁷ While the financial sector led the efforts to monetize Aadhaar, many other industries continue to follow suit (e.g, with “technology stacks” for healthcare, lending, telemedicine, and agriculture).³⁸

30 See “United Payments Interface,” February 2015, <https://archive.vn/xZEW0#selection-3321.29-3327.29>.

31 A switch handles authentication and communication between issuing and acquiring banks.

32 A landscaping study of companies built on top of India Stack recorded at least 150 startups doing background verification, digital lending, and digital wallets as far back as 2018. Bharat Inclusion Fund, “Startups building on IndiaStack: A Landscaping Study,” Medium, August 23, 2018, <https://medium.com/bharatinclusion/startups-building-on-indiastack-a-landscaping-study-a77344b51d19>.

33 UIDAI provided blueprints for how its architecture may be used for financial-sector commercial products to the Reserve Bank of India (RBI). See “Report of Task Force on an Aadhaar-Enabled Unified Payment Infrastructure,” February 2012, <https://archive.org/details/reporttaskforceaadhaarpaymentinfra>. Indeed, RBI leadership in charge of developing standards for payments and settlements included industry players behind Aadhaar. See Anuj Srivas, “Exclusive: How the RBI Forced National Payments Body to Hire Government Favourite as CEO,” *The Wire*, February 14, 2018, <https://thewire.in/business/rbi-npci-digital-india>. The committee set up for “deepening digital payments” was helmed by the first chairperson of the UIDAI, Nandan Nilekani. See Aria Thaker, “Behind RBI’s Digital Payments Panel, a Controversial Firm’s Shadow, Conflict of Interest Allegations,” *Scroll.in*, January 10, 2019, <https://scroll.in/article/908802/behind-rbis-digital-payments-panel-a-controversial-firms-shadow-conflict-of-interest-allegations>.

34 Aria Thaker, “The New Oil: Aadhaar’s Mixing of Public Risk and Private Profit,” *Caravan*, April 30, 2018, <https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit>.

35 See Suprita Anupam, “Nandan Nilekani on Creating the Architecture for India’s Digital Future,” *Inc42*, April 24, 2019, <https://inc42.com/features/nandan-nilekani-on-aadhaar-digital-india-kyc-gst-upi-payments-fastag/>. See also ProductNation/iSPIRT, “Nandan Nilekani: Identity, Payments, Data Empowerment 2019,” SlideShare, December 9, 2019, <https://www.slideshare.net/ProductNation/nandan-nilekani-identity-payments-data-empowerment-2019>; and ITU News, “Aadhaar: India’s Route to Digital Financial Inclusion,” June 26, 2017, <https://news.itu.int/aadhaar-indias-route-to-financial-inclusion/>; and Ronald Abraham et al., “State of Aadhaar Report 2016–17, Chapter 4: Financial Inclusion,” Omidyar Network, May 2017, <https://static1.squarespace.com/static/5b7cc54e4eb7d25f7af2be/t/5bc535e324a694e7994fcf0c/1539651143095/State-of-Aadhaar-Ch4-Financial-Inclusion.pdf>.

36 See ProductNation/iSPIRT, “Nandan Nilekani: Identity, Payments, Data Empowerment 2019.”

37 For example, according to economist and author M. S. Sriram, issues of identity, deduplication, and authentication were not the most significant barriers to financial inclusion. See Sriram, “Moving Beyond Aadhaar: Identity for Inclusion,” *Economic & Political Weekly* 49, no. 28 (July 12, 2014), <https://www.epw.in/journal/2014/28/special-articles/identity-inclusion.html> (paywall).

38 For healthcare, see “National Health Stack: Strategy and Approach,” July 2018, https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Documents-for-consultation.pdf; and Seema Singh and Arundhati Ramanathan, “The Elite VC-Founder Club Riding Aarogya Setu to Telemed Domination,” *The Ken*, May 18, 2020, <https://the-ken.com/story/the-elite-vc-founder-club-riding-aarogya-setu-to-telemed-domination/>. On loans for MSME, see Arundhati Ramanathan, “Sahay, India’s Fintech Disruption Sequel,” *The Ken*, May 8, 2020, <https://the-ken.com/story/sahay-indias-fintech-disruption-sequel/>.

Agile Regulation Keeps the Ecosystem Alive¹

As private-sector use of Aadhaar took off, many harms materialized³⁹ and several entities submitted petitions to challenge the law.⁴⁰ Even as the Supreme Court struck down private-sector uses of Aadhaar in 2018,⁴¹ and dealt an existential blow to entire sectors⁴² built with its affordances, in practice this did not ultimately limit companies from using Aadhaar for private gain.

As if seeing the Supreme Court's verdict as a procedural complication and not a principled opposition to private use, the Ministry of Law and Justice introduced an ordinance amending the Aadhaar Act and other finance laws to keep authentication possibilities alive by introducing "offline verification" and "alternative virtual identity."⁴³ This allowed Aadhaar number holders to produce digitally signed copies of their Aadhaar acknowledgement letter by producing a QR code or .xml file downloaded from the UIDAI website.⁴⁴ Despite these shoddy and dangerous accommodations, businesses were still disgruntled, as the ease and low costs of verification were nevertheless affected.⁴⁵

In response, the Central Government issued a note to allow private entities to use Aadhaar-based verification facilities upon the fulfillment of certain conditions, and at the discretion of UIDAI and the appropriate regulator.⁴⁶ With this cue, the finance-sector regulator allowed the use of Aadhaar for opening bank accounts,⁴⁷ and UIDAI allowed private firms to regain access to Electronic Know Your Customer (eKYC) authentication.⁴⁸

39 E.g., through the profiling of blue-collar workers, or fraudulent uses of data. See Usha Ramanathan, "The Future Is Here: A Private Company Claims It Can Use Aadhaar to Profile People," *Scroll.in*, March 16, 2016, <https://scroll.in/article/805201/the-future-is-here-a-private-company-claims-to-have-access-to-your-aadhaar-data>; and "UIDAI Suspends Airtel, Airtel Payments Bank's e-KYC License over Aadhaar Misuse," *Economic Times*, December 16, 2017, <https://economictimes.indiatimes.com/news/politics-and-nation/uidai-suspends-airtel-airtel-payments-banks-e-kyc-licence-over-aadhaar-misuse/articleshow/62096832.cms>.

40 For example, activists challenged the linking of Aadhaar to bank accounts and mobile numbers. See Laxmi Prasanna, "New Petition in Apex Court Challenges Linking Aadhaar with Bank Account and Phones," *Times of India*, October 19, 2017, <https://timesofindia.indiatimes.com/india/new-petition-in-apex-court-challenges-linking-aadhaar-with-bank-account-and-phones/articleshow/61145283.cms>. See also Anoo Bhuyan, "Aadhaar Isn't Just about Privacy. There Are 30 Challenges the Govt Is Facing in Supreme Court," *The Wire*, January 18, 2018, <https://thewire.in/government/aadhaar-privacy-government-supreme-court>.

41 Justice K. S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012, https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf.

42 Komal Gupta, "Aadhaar Verdict Puts Fintech Firms in a Spot," *Livemint*, September 28, 2018, <https://www.livemint.com/Politics/gIGcFQMgHR146zXfPkGqjO/Aadhaar-verdict-puts-fintech-firms-in-a-spot.html>.

43 Anita Baid, "RBI Amends KYC Master Directions: Aadhaar to Be Officially Valid Document Now," *Moneylife*, May 31, 2019, <https://www.moneylife.in/article/rbi-amends-kyc-master-directions-aadhaar-to-be-officially-valid-document-now/57317.html>.

44 Ministry of Law and Justice, "The Aadhaar and Other Laws (Amendment) Ordinance, 2019," https://uidai.gov.in/images/news/Ordinance_Aadhaar_amendment_07032019.pdf. See also UIDAI, "Secure QR Code Specification," March 2019, https://uidai.gov.in/images/resource/User_manual_QR_Code_15032019.pdf. Note that the supposed security features of a digital identity linked to biometrics is undone when the artifact of proof of identity becomes part of an .xml file.

45 Pratik Bhakta, "India's Fintech Companies Struggle for an Alternative to Aadhaar," *Economic Times*, December 21, 2018, <https://economictimes.indiatimes.com/small-biz/startups/features/indias-fintech-companies-struggle-for-an-alternative-to-aadhaar/articleshow/67186586.cms>.

46 Pratik Bhakta, "Soon, Non-Banking Companies May Verify via eKYC," *Economic Times*, May 17, 2019, <https://economictimes.indiatimes.com/industry/banking/finance/banking/soon-non-banking-companies-may-verify-via-ekyc/articleshow/69366383.cms>.

47 "Banks Can Use Aadhaar for KYC with Customer's Consent: RBI," May 29, 2019, <https://economictimes.indiatimes.com/industry/banking/finance/banking/banks-can-use-aadhaar-for-kyc-with-customers-consent-rbi/articleshow/69568435.cms>.

48 This was based on a creative interpretation of the opinion of the attorney general. For example, authentication functions were allowed for purposes of welfare delivery. UIDAI applied this as if products using Aadhaar-enabled Payments System (AePS) could access it, since AePS might be used in the course of welfare delivery.

REMAKING REGULATION IN TECHNOLOGY'S IMAGE¹

Regulatory practice surrounding Aadhaar indicates that regulation is becoming beholden to the same values, managerial styles, procedural cadence, interests, and language of communication as the applications of technologies it seeks to regulate.²

*Regulation as Public Relations and Marketing*³

For the first seven years of its existence, Aadhaar had little oversight and was shaped by UIDAI, a body preoccupied with the market importance of Aadhaar. Even after the passage of the law, regulation and technology development have worked hand-in-hand to create and maintain the conditions for use of the biometric data by private companies, to the artificial exclusion of socioeconomic concerns.⁴⁹ Regulations not only consolidated the developments of the first seven years of the project, but also presented a revisionist history of the actual goals of the project, obscuring the stakes for private interests.⁵⁰ For this and other reasons, many of the problems with Aadhaar should not be understood as *failures* of law or regulation, but as *products* of law and regulation.

While law and regulation were meant to address the risks of Aadhaar, the instruments uncritically adopted disingenuous jargon like “financial inclusion,” “innovation,” and “efficiency.” What was righteously proclaimed by UIDAI as public buy-in for the project owed some credit to incentives provided to enrollment agencies,⁵¹ as well as expertise drawn from “multiple areas of marketing, creative communication, research, understanding of past social marketing efforts, media channels, branding and positioning.”⁵²

*Regulation as Technology Product*⁶

The private sector's direction and influence in the development and adoption of technology projects has a key feature of anticipating concerns around data use, and making data protection itself a product, feature, and layer.⁷

49 Law and regulation of the finance sector, for example, creates an artificial distinction between civil and political rights (often framed in the narrow language of privacy) and economic imperatives (generalized benefits for the country). See also Nandan Nilekani, “Data to the People: India's Inclusive Internet,” *Foreign Affairs*, September/October 2018, <https://uidai.gov.in/images/news/Data-to-the-people-Nandan-Nilekani-foreign-affairs.pdf>.

50 See Ramanathan, “The Future Is Here: A Private Company Claims It Can Use Aadhaar to Profile People,” *Scroll.in*.

51 Anand Venkatanarayanan, “How Trustworthy Are the Entries in the Aadhaar Database?” *MediaNama*, September 28, 2017, <https://www.medianama.com/2017/09/223-how-safe-is-the-aadhaar-database/>.

52 UIDAI, “Aadhaar Awareness and Communications Strategy Advisory Council Order,” February 17, 2010, <https://archive.org/details/UIDAIMediaAwarenessAdvisoryCouncil/page/n1/mode/2up>. See also conflicts of interest within initiatives like ID4D. Transnational interests like the World Bank's ID4D initiative, pushing digital identification in the language of rights to developing countries, even as its composition reveals shocking conflicts of interests, including investors in fintech and related data economy businesses, venture capitalists as well as Nandan Nilekani himself. See also Anandita Thakur and Karan Saini, “Selling Aadhaar: What the UIDAI's Advertisements Don't Tell You,” *The Wire*, August 23, 2018, <https://thewire.in/rights/aadhaar-advertisements-identity-citizenship-rights>. “If the advertisements espoused by the UIDAI were to be believed, the prospect of biometric failures and internet connectivity issues do not even figure into the day-to-day business of the coercive practice of making Aadhaar an unsubstitutable instrument of citizen life in India.”

In the case of Aadhaar and data governance in India, the private-sector group building India Stack took it upon itself to “innovate” around encoding data-protection safeguards (e.g., through “consent” and “transparency”) within the technology ecosystem and to solve for data protection. This maneuver simultaneously tries to foreclose demands for a data-protection law (which India does not have) and, more importantly, *distracts* from broader questions about whether such datafication is at all necessary and who benefits from it, making the present trajectory seem inevitable.

Consent: Arguably one of the biggest issues with Aadhaar has been its coercive nature and absolute disregard for consent, which has continued to be an issue even after courts have attempted to intervene.⁵³ Perhaps learning from the problems caused by the pesky need for consent, India Stack evolved a “consent layer”⁵⁴ consisting of two products: Account Aggregator and Data Empowerment and Protection Architecture (DEPA).⁵⁵ The former is an entity legally instituted by the Reserve Bank of India, which is tasked with consolidating, organizing, and retrieving data about a customer’s different types of financial arrangements, including mutual funds and insurance schemes. The latter aims to provide “a modern privacy data sharing framework” and introduces *convenience* into the process of sharing personal data in exchange for finance, healthcare, and other services by building an interface for the purpose. The contents of this layer effectively make consent a bureaucratic formality and logistical complication to be simplified by technology, obscuring the instrumentalization of people’s lives toward value creation for private firms.

The consent-related products blindside the need to consider whether such datafication is at all necessary, or what the subsequent terms of use of this data might be, ultimately cornering regulation into becoming a mimicry of the direction the market for data takes.

Transparency: The Aadhaar project documents are littered with references to the importance of transparency. One of the main sources of proactive disclosure about Aadhaar is the UIDAI dashboard,⁵⁶ where monthly data about enrollments, updates, and authentication are maintained. However, this data is a far cry from the granularity or consistency of useful information that people have been demanding for a long time,⁵⁷ like the number of failed biometric authentications.

The transparency-related artifacts use aesthetic devices like dashboards, data visualizations, and social media campaigns that have little substance and remain inert to demands for meaningful information.

53 Anuj Srivas, “Aadhaar Moves Forward as Ministries Navigate SC Order and Public Backlash,” *The Wire*, September 20, 2016, <https://thewire.in/government/aadhaar-supreme-court-compliance>.

54 Jayadevan PK, “Consent, the Final Layer in India’s Ambitious Data Regime, Falling in Place,” *Factor Daily*, September 5, 2017, <https://factordaily.com/consent-architecture-indiastack/>.

55 See IndiaStack, “About Data Empowerment and Protection Architecture (DEPA),” <https://www.indiastack.org/depa/>.

56 See UIDAI, Aadhaar Dashboard, https://uidai.gov.in/aadhaar_dashboard/.

57 See Gus Hosein and Edgar Whitley, “Identity and Development: Questioning Aadhaar’s Digital Credentials” in *Dissent on Aadhaar*.

Regulation as Optimization¹

The regulatory framework around Aadhaar has been perennially agile and adaptive to the needs of the data economy. Within the broader vision for technology-enabled governance, agencies are encouraged to roll out projects “as soon as possible, and iterated rapidly, rather than waiting to roll out a perfect system.”⁵⁸

Besides aligning regulatory priorities with the workflows and cultures of technology firms, there is a push for regulatory practice to adopt the same logics (prediction, optimization) as technology directions within the industry. For example, Nandan Nilekani argues that the market is a perfectly responsive system: “Digital systems enable early-warning systems and more precise regulatory interventions, e.g., for managing loan defaults.”⁵⁹

CONCLUSION⁴

The data economy relies on instituting individuals as data points within databases. Law and regulation around Aadhaar cooperate to create the perfect conditions under which this might be possible: architecting biometric information as truth, and facilitating its use, integration, and maintenance within other systems. Even then, law and regulation maintain a depoliticized reading of economic enrichment from data, and a false dichotomy between questions of rights and questions of enrichment.

Instead of treating biometric information simply as data to be guarded, law and regulation should reckon with the entire range of powerful market interests that the networked subject kicks into motion, as well as regulation’s own malleability in the face of these forces.

58 Ministry of Finance, “Report of the Technology Advisory Group for Unique Projects,” January 31, 2011, https://www.finmin.nic.in/sites/default/files/TAGUP_Report.pdf.

59 See ProductNation/iSPIRT, “Nandan Nilekani: Identity, Payments, Data Empowerment 2019.”

A First Attempt at Regulating Biometric Data in the European Union¹

Els Kindt (KU Leuven)²

INTRODUCTION³

In 2004, the European Union (“Union”) enacted legislation that obligated Member States (“MS”) to store facial images and fingerprints in citizens’ passports and travel documents.¹ Around the same time, the Union set up large-scale databases containing the biometric data of asylum and visa seekers and an information system for protecting the Schengen Area.² It wasn’t long before this spilled over into public and private entities, which began using biometric data for crowd control, access control in the workplace, and monitoring in schools. While acknowledging that the use of biometric technology has many potential benefits, the Council of Europe warned that biometric data should be considered as “sensitive” data that presents risks, because it contains information about health and race, has the ability to identify people, can make it easier to link records, and is irrevocable.³

¹ EU Regulation No 2252/2004, December 13, 2004.

² Consider, for example, Eurodac, the Visa Information System (VIS), and the Schengen Information System (currently SIS II), which all emerged after 2000. Biometric data remains central to the Union’s information systems, including the European Travel Information and Authorisation System (ETIAS), the Entry/Exit System (EES) (Regulation No 2017/2226), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), as is clear from the recent interoperability framework (Regulation No 2019/817 and Regulation No 2019/818).

³ See Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (Strasbourg: 2005), and the updated Progress Report of 2013, T-PD(2013)06, <https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81>. The Council of Europe adopted the European Convention on Human Rights in 1950, and the Convention No. 108 on data protection in 1981, as revised in 2018 (Convention No. 108+). The Council of Europe consists of forty-seven Member States and is distinct from the European Union.

Despite the risks, the general data-protection framework and most national legislation did not contain specific provisions on biometric data use and processing,⁴ and guidance remained limited while these technologies were being developed.⁵ To address these gaps, some national supervisory data protection authorities (SAs) developed frameworks for biometric use.⁶ As part of these frameworks, SAs have focused on the sensitive nature of the data, the risks of maintaining databases, and the possibility of “function creep.”⁷ The SAs also focused on whether the use of biometrics was proportionate to the legitimate aim sought to be achieved (i.e., the “proportionality principle”), leaving much room for discretionary policy considerations and unpredictable outcomes when applying the proportionality principle.⁸

It was against this backdrop that the Union introduced the General Data Protection Regulation 2016/679 (GDPR) in 2016. The regulation is directly applicable in Member States and includes provisions for both public and private biometric data processing. The Union also introduced Directive 2016/680 (Data Protection Law Enforcement Directive, or DP LED), which applies specifically to personal data processing for the prevention, detection, investigation, or prosecution of crime by law enforcement authorities (LEAs).

THE EU’S REGULATORY APPROACH TO BIOMETRIC DATA PROCESSING

Both the GDPR and DP LED provide, for the first time, a definition of biometric data: “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural

4 See Directive 95/46 and Framework Decision 2008/977/JHA. “Processing” is understood very broadly, and is defined as “any operation or set of operations . . . whether or not by automated means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (Article 4(2), GDPR). Only a few Member States introduced specific legal provisions, e.g., France, Article 25 and 27 Act No. 78-17.

5 See e.g., the Article 29 WP, Working Document on Biometrics 2003 (WP 80), Opinion 2/2012 on facial recognition in online and mobile services (WP192), and Opinion 3/2012 on developments in biometric technologies (WP193).

6 This is done by advising, adopting opinions, and issuing guidelines, authorizations, restrictions, and bans. See, e.g., for France, Claire Gayel, “The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL’s Deliberations,” *Computer Law & Security Review* 32, no. 3 (June 2016), 450–461, <https://doi.org/10.1016/j.clsr.2016.01.013>.

7 This can happen, for example, when an agency uses the data for something other than its original purpose (e.g., for law enforcement purposes). See also CNIL, “Communication de la CNIL relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données,” Communication central storage fingerprint, December 28, 2007, <https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf>.

8 The proportionality principle is an important principle in data-protection legislation. It requires that the processing is lawful and the data adequate and relevant and not excessive for the purpose specified. When interfering with human rights, the proportionality principle requires in addition a three-step test: that there is accessible and sufficiently certain law allowing the interference (“rule of law”); a legitimate aim; and *necessity in a democratic society*. For assessing the latter, one needs to determine whether (1) the interference answers a “pressing social need,” (2) the argued reasons for deploying the interference are relevant and sufficient, and last but not least (3) whether all of this, in particular the interference (in our case the use of biometric technology), is in proportion with the legitimate aim pursued. As there remained confusion about the need for double review and because there was also lack of clarity about the three-pronged approach, this resulted in divergent and unpredictable outcomes when applying the proportionality principles and in broad “margins of appreciation.” See also E. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Dordrecht: Springer, 2013), 403 et seq. and 621 et seq.

person, such as facial images or dactyloscopic [fingerprint] data.”⁹ A particularly noteworthy aspect is the “specific technical processing”¹⁰ component, which effectively excludes “raw” data stored and retained in databases (e.g., of facial images captured on CCTV, voice recordings, or fingerprints),¹¹ or when published on a website or social network. The GDPR accounts also mention that the “processing of photographs should not systematically be considered to be processing of special categories of personal data...”¹² Video footage of an individual is also not considered biometric data as long as it has not been specifically technically processed in order to contribute to the identification of the individual.¹³

While the GDPR states that “processing of biometric data for the purposes of uniquely identifying”¹⁴ is prohibited,¹⁴ there are many exceptions to this prohibition, including when the data “are manifestly made public” or if processing is “necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.”¹⁵ Because the exceptions remain vague (e.g., “substantial public interest”) and are numerous,¹⁶ the GDPR still allows the processing of biometric data in many circumstances, including those where people give explicit consent.¹⁷ Finally, the GDPR specifies that Member States may maintain or introduce further conditions or limitations.¹⁸

9 Article 4(14) GDPR and Article 3(13) Directive 2016/680. The technical process is likely to be understood as a biometric technical processing. The original definition in the EU Commission's GDPR proposal of January 25, 2012 COM(2012) 11 final and in the European Parliament's position in its first reading of April 13, 2014 was broader: “biometric data” means any [personal data] relating to the physical, physiological, or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data” (Article 4(11)). Experts view this definition as narrow and contrary to a general understanding of biometric data. For examples, see the ISO/IEC 2382-37 Information Technology—Vocabulary—Part 37: Biometrics (2017), where “biometric data” (3.3.6) includes both biometric samples (analog or digital representations of biometric characteristics), hence the initial or “raw” data, and the technically processed data thereof. See also EES, where biometric data is defined as including images: “biometric data” means fingerprint data and facial image” (Regulation 2017/2226, article 3.1 (18)). On the biometric terminology and possible confusion, see also Catherine Jasserand, “Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data,” *EDPL* 2, no. 3 (2016): 297–311, <https://doi.org/10.21552/EDPL/2016/3/6>.

10 Added by the Council of the Union, composed of the heads of the Member States and governments. See Council doc. 15395/14, December 19, 2014, <https://www.statewatch.org/media/documents/news/2014/dec/eu-council-dp-reg-15395-14.pdf>. This modification was requested and added to the initially proposed definition and finally adopted. On the origin of this modification, see E. J. Kindt, “Having Yes, Using No? About the New Legal Regime for Biometric Data,” *Computer Law & Security Review* 34, no. 3 (June 2018): 523–538, <https://doi.org/10.1016/j.clsr.2017.11.004>. This article also contains a graphic showing what counts as biometric data and not, and which legal provisions apply.

11 For example, the collection of facial images by governments to issue identity documents, and their storage in databases.

12 Rec. 51 GDPR. See also EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices, on Video Surveillance*, January 29, 2020, § 74 (“EDPB Guidelines 3/2019 on video devices”).

13 Ibid.

14 Article 9.1 GDPR. The general prohibition was an amendment requested by the European parliament (EP) to the original proposal of the EU Commission. The processing of biometric data was hereby hence added to the list of special categories of data. EP first reading, T7-0212/2014, March 12, 2014. This followed the 2012 suggestions of the Council of Europe's Consultative Committee working on the modernization of Convention No. 108. Compare with Article 6.1 of Convention 108+ of the Council of Europe. The words “for purposes of uniquely identifying” were added later during the trilogue in 2016. See Council position, 05419/1/2016, April 8, 2016.

15 There are ten explicit exemptions. See Article 9.2 GDPR, “Processing of Special Categories of Personal Data,” <https://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm>.

16 The exception “personal data which are manifestly made public by the data subject” is also much debated. See also, e.g., EDPB Guidelines 3/2019 on video devices, § 70.

17 For example, banks may rely on biometric data for financial account access if their customers explicitly agree.

18 Article 9.4 GDPR. For example, the Netherlands adopted a law allowing biometric data processing if necessary for “authentication or security purposes.” Article 29 Dutch GDPR implementation Act of May 16, 2018. The Dutch SA however seems to apply this in a strict manner: see the decision of the Dutch SA (Autoriteit Persoonsgegevens), December 4, 2019, imposing a fine of 725,000 euros for unlawful fingerprinting of employees for access control (appeal pending), available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_vingerafdrukken_personeel.pdf (in Dutch).

Under the DP LED, LEAs do not face a prohibition and may process biometric data to uniquely identify people where strictly necessary, subject to appropriate safeguards, and only in three situations: if authorized by law, to protect vital interests, or where the processing relates to data manifestly made public by the data subject.¹⁹ While the DP LED has data processing restrictions only if there is “specific technical processing,” LEAs may collect data (e.g., facial images or voice recordings) without biometric specific limitations imposed by the DP LED.

In cases where new technologies lead to processing that is “likely to result in a high risk” or in case of large-scale processing of special categories of personal data, the GDPR and DP LED require entities to conduct Data Protection Impact Assessments (DPIA). A DPIA is also required for systematic monitoring of a publicly accessible area on a large scale.²⁰ DPIAs mandate entities to conduct a comprehensive assessment of the risks of processing, as well as of the necessity and proportionality of the technology.²¹ In some cases, private or public entities will have to ask the SA for prior consultation and authorization.²² Furthermore, if the biometric data processing interferes with fundamental human rights and freedoms, including the right to privacy and the right to personal data protection, the fundamental rights framework shall be applied as well.²³

The following sections outline the key learnings from these regulatory attempts, discuss their effectiveness, and highlight learnings for future regulation.

ASSESSMENT AND EFFECTS OF THE REGULATORY CHOICES

Impact of Definitional Choices

Since the GDPR and DP LED definitions of biometric data require “specific technical processing,” the collection and storage of data like facial images or voice recordings do not receive more or stricter protection than any other personal data, such as the requirement of explicit consent or necessity and

19 See Article 10 Directive 2016/680. Note that in the two last situations, the need for an authorizing law doesn’t seem to be required. For “data manifestly made public by the data subject,” this is meant to cover social media.

20 Article 35 GDPR and Article 27 Directive 2016/680. This DPIA requirement was part of the original EU Commission’s GDPR proposal of January 25, 2012 COM(2012) 11 final.

21 While the DPIA requirement adds important responsibility (and liability) for assessing the risks, necessity, and proportionality of biometric systems, post-GDPR experience already shows that such assessment is in general very difficult to conduct in practice. For the French SA’s guidance, see CNIL, “The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment” and its updates, June 25, 2019, <https://www.cnil.fr/node/23992>.

22 See, e.g., CNIL (French SA), “Délibération no. 2019-001,” January 10, 2019, <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf>. The document discusses the processing of employee biometric data for access control to premises, devices, and apps at work, which requires such DPIA, Article 11.

23 See Kindt, *Privacy and Data Protection Issues*, 570 et seq; see also supra note 8 on the proportionality principle. The relevant fundamental rights of the European Convention on Human Rights and of the EU Charter that could be affected by biometric technology include, besides the right to privacy and data protection, the right to freedom of expression and of free movement, non-discrimination, and the right to assembly. In relation to LFR and LEAs, see FRA, “Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, November 27, 2019, <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>. See also Pete Fussey and Daragh Murray, “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology,” The Human Rights, Big Data and Technology Project, July 2019. National traditions interpreting these fundamental rights must also be taken into account, adding complexity to the matter.

the need for law as required under Article 9.2 GDPR. It is the use of the data, rather than its sensitive nature or its ability to enable identification, that determines when data becomes biometric.²⁴

Because of the way the definition was written, the risks of biometric data collection are not covered. Data that should get special protection does not, because it is not currently being processed. This is particularly concerning because later use, particularly by law enforcement agencies, may be less transparent or restricted, and the data could be used without any notice to the individuals concerned or to the public.²⁵ Under the permissions granted under the GDPR and the DP LED, this implies that companies and government can collect large databases of images (e.g., similar to the information collected by Clearview), which might later be used for law enforcement purposes.²⁶

Finally, the definition is not in line with the European Court of Human Rights case law, which has repeatedly stated that the practice of capturing, collecting, and storing unique human characteristics in databases interferes with the right to respect for private life.²⁷ Such interference was confirmed for facial images in *Gaughran v. The United Kingdom*, where the Court took facial recognition and facial mapping techniques into account, and “found that the retention of the applicant’s DNA profile, fingerprints and photograph amounted to an interference with his private life.”²⁸

An appropriate definition should offer legal protections to unique human characteristics that are fit for identification purposes or could be used by automated processes, and regulation should also restrict the storage of this data in databases.²⁹ An alternative definition of biometric data could be: “all personal data (a) relating directly or indirectly to unique or distinctive biological or behavioural characteristics of human beings and (b) used or fit for use by automated means (c) for purposes of identification, identity verification, or verification of a claim of living natural persons.”³⁰

Lack of Clarity around Biometric “Prohibition” and Sweeping Exceptions

The law should take into account how different biometric systems function, and these functionalities should be regulated depending on how the data is processed. For example, while prohibitions on use and processing are outlined in the law, Article 9.1 GDPR does not distinguish between one-to-one (1:1) biometrics comparisons (i.e., verification), and one-to-many (1:n) comparisons (i.e., identification).³¹

24 The definition of biometric data does not include so-called “soft” biometrics, such as emotions, since they usually do not allow for identification or identity verification.

25 Article 23 GDPR allows Union or MS law to restrict the rights of data subjects, including the right to information, e.g., to protect public security. See also Article 13.3 Directive 2016/680.

26 For example, LEAs could use FR technology combined with social media profiles; or see the online dating investigation tool offered by Socialcatfish.com, which has commercialized social media and dating profile data.

27 ECtHR, *S. and Marper* 2008, § 86; ECtHR, *M.K. v France* 2013, § 26; see also Cons. const. (France) no. 2012-652, March 22, 2012 (*Loi protection de l’identité*), § 6.

28 ECtHR, *Gaughran v. The United Kingdom* 2020, §70.

29 This should come first and in addition to a prohibition to use for identification purposes, except for precise limited exceptions determined by law.

30 See also Kindt, 2013, *Privacy and Data Protection Issues* 144 et seq. and 851 et seq.

31 See and compare the wording of the prohibition with the definition of article 4(14) GDPR, which refers to the two functionalities (“which allow or confirm the unique identification”): article 9 GDPR forbids only “biometric data for the purpose of uniquely identifying,” leaving it uncertain if this prohibition also includes processing for purposes of confirming identification (verification).

Meanwhile, the Council of Europe and SAs have stated that biometric verification contains less risk¹ than biometric identification because no database is needed.³²

On the other hand, one-to-many comparisons (i.e., identification) introduce additional risks,² including the large-scale collection and storage of biometric information in databases, probability-based matching (which raises concerns about accuracy and false positives), and privacy-surveillance concerns. Because the GDPR and DP LED do not differentiate between the two functionalities, there is legal uncertainty for companies that want to invest in biometric verification technologies and privacy-enhancing methods.³³ Appropriate regulation should meaningfully address the relative risks of each functionality, discouraging or banning those that pose real risks, and potentially encouraging those that have the potential to offer real privacy and security protections.

Finally, the broad exceptions and overall vagueness of the law leaves the door open for specifically risky uses of biometric data like live facial recognition (LFR). The GDPR exceptions are general, and include language allowing biometric data processing for “reasons of substantial public interest” based on law. Because of the way this and other exceptions are worded, it remains unclear whether these serve as a legal basis that authorizes public or private entities to deploy LFR (e.g., at large stadium events).³⁴ The GDPR and DP LED alone will not resolve these questions, and additional specific EU and national laws are needed.³⁵

CONCLUSION⁴

The GDPR and DP LED approaches to defining biometric data exclude the collection of so-called “raw” data like facial images, yet protection is most important at the initial stage of the creation of biometric systems and infrastructures. The GDPR and DP LED also deviate from Europe’s human rights case law and its own approach to data “processing,” which is that data protection should start at the collection stage. A comprehensive legal framework should also aim to restrict⁵

32 CoE, Progress Report 2013 (supra note 3), 58 (recommendation 7, as set out in the CoE report of 2005); Article 29 WP, WP 80 (supra note 5), 11 (Conclusion). One shall hence keep in mind that it is precisely the use of databases against a general public in public places (or in places accessible to the public, such as shops) and the identification functionality that pose the most risk, e.g., of surveillance or of unwanted identification. For example, verification could use local storage and strict safeguards that offer increased security for people trying to access phones or bank accounts, e.g., by local comparison of a facial image locally stored in a protected template form under the individual’s control, e.g., on a smartphone, for controlling access to a payment application. Verification and identification have also been rightly distinguished by data protection authorities such as the French SA: see CNIL, “Communication central storage fingerprint,” December 28, 2007, 5–6.

33 Such methods exist, in particular template-protection methods, permitting pseudonymous, revocable, and unlinkable biometric identifiers. See also CoE, Progress Report 2013 (supra note 3), 30–31 and Kindt, *Privacy and Data Protection Issues*, 801–807. Because of the data-protection-by-design obligation, such methods are very important.

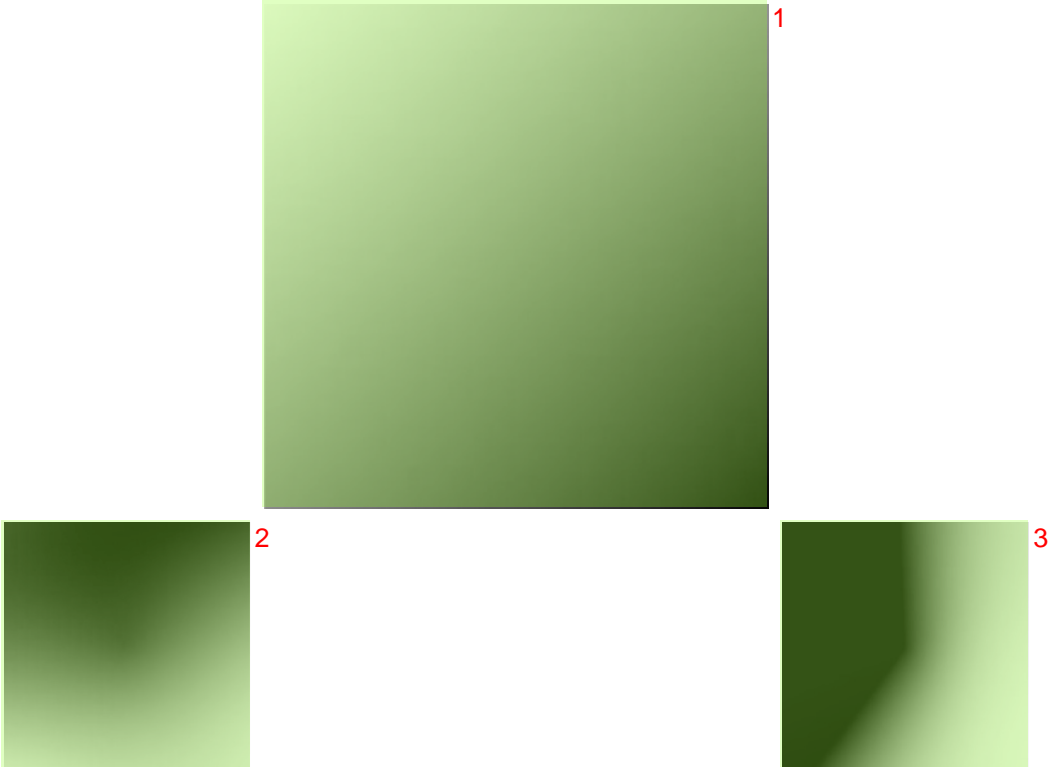
34 See Danish SA, “Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion,” May 24, 2019, <https://www.datatilsynet.dk/tilsyn-og-afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-brondby-stadion/>.

35 Any interference with fundamental rights and freedoms requires a law that shall be sufficiently precise and certain (foreseeability) and accessible, in order to exclude arbitrariness. This is especially important for technology because “the technology available for use is continually becoming more sophisticated” (ECtHR, *Kruslin*, 1990, §33, on voice recording in criminal proceedings). In COVID-19 times, public controllers and LEAs may also be tempted to deploy LFR for controlling movement restrictions. Because of the risks posed for fundamental rights, the EU Commission recently launched a debate about possibly additional legislation for remote biometric identification: see EU Commission, White Paper on Artificial Intelligence: a European Approach to Excellence and Trust, February 19, 2020, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

any biometric data storage in databases, and should offer clear guidance as to any undesirable or forbidden biometric identification, unless allowed under strict legal conditions, and biometric verification solutions, under precise conditions. More precise laws around police collection and use of such data and policing techniques are needed, in addition to a strict interpretation of the necessity and proportionality tests as they apply to law enforcement use. ¹

Apart from stronger legal and procedural safeguards under the GDPR and DP LED, and enhanced consideration of the fundamental rights' three-steps test, policymakers should adopt special regulation to strengthen and reinforce fundamental rights. These could include bans or moratoria against particular uses of biometric technology like LFR unless strictly necessary and proportionate for substantial public interests described in law. This is crucial, especially if LFR directly contradicts and affects the essence of fundamental rights, such as the right to peaceful assembly, which should not be left to case-by-case assessment. ²

As other states or countries look to the Union for guidance around regulating biometric data collection and use, this chapter has aimed to highlight the challenges posed by uncritically adopting the text of the GDPR and DP LED. For any future legislation, it will be important to recognize the risks and functionalities of biometric data systems, starting from the collection and storage of the data, not just during its processing or use, and to reconsider broadly worded exceptions that provide loopholes for companies, governments, and authorities to exploit. ³



Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases¹

Ben Hayes (AWO agency, Consultant legal advisor to the ICRC)²
Massimo Marelli (Head of the ICRC Data Protection Office)

The International Committee of the Red Cross (ICRC) works with some of the most vulnerable people in the world, providing humanitarian assistance to populations affected by armed conflict and other situations of violence.¹ Like many other humanitarian organizations, the ICRC is exploring new technologies to support its operations and beneficiaries. As part of its digital transformation agenda, the ICRC developed a Biometrics Policy ("the Policy") that both facilitates the responsible use of biometrics and addresses data-protection challenges. ICRC adopted the Policy in August 2019,² which recognizes the legitimacy and value of using biometrics to support its programmatic and operational objectives while also ruling out the creation of any central, biometric databases in the short term. This article discusses some of the factors brought to bear on the decision-making process we went through as an institution.³

¹ International Committee of the Red Cross, "The ICRC's Mandate and Mission," <https://www.icrc.org/en/mandate-and-mission>.

² International Committee of the Red Cross, "The ICRC Biometrics Policy," October 16, 2019, <https://www.icrc.org/en/document/icrc-biometrics-policy>.

³ This article builds on Ben Hayes and Massimo Marelli, "Facilitating innovation, ensuring protection: the ICRC Biometrics Policy," ICRC, *Humanitarian Law & Policy*, October 18, 2019, <https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy>.

BIOMETRICS IN THE HUMANITARIAN SECTOR¹

The ICRC works in more than ninety countries and is part of a global humanitarian network of over eighty million people.⁴ It provides healthcare, food, basic shelter, clothing, access to education, employment, and assistance to detained persons, and also helps restore family links by reuniting separated persons and finding missing persons. To address the logistical challenges of protection and assistance programs, some humanitarian organizations use biometric identification systems to enroll people in humanitarian programs and verify their identity when providing services or assistance. The primary justification for this use is that recipients of humanitarian assistance frequently lack identity documents, which poses a challenge if they need to be identifiable.

Humanitarian organizations have intensely debated when and how people “need” to be identifiable, and the legitimacy of using biometrics to perform that function.⁵ On one side, continuity of healthcare and some forms of humanitarian assistance clearly need people to be identifiable (e.g., for provision of travel documents or financial services). For example, the United Nations Refugee Agency (UNHCR) has a clear mandate to identify refugees and asylum seekers, and to provide them with identity documents⁶ (though it has been heavily criticized for deploying biometrics⁷). However, most humanitarian organizations do not have a formal mandate to provide people with an identity or supporting documentation. They have primarily developed and implemented biometric ID systems because of the perceived efficacy and accountability gains such systems provide.⁸

While existing ID cards, social security numbers, and other documents may be used by humanitarian organizations to check or verify an individual's identity, these cannot be unequivocally associated with a single individual in the way that a biometric ID can. Biometric databases can also be used to prevent the same individual from registering in an aid program more than once, which is attractive for humanitarian organizations that are concerned about individuals or families obtaining more assistance than has been earmarked for them.⁹ Indeed, biometrics have played an increasingly large role in the scaling up of cash-transfer programs (CTPs).¹⁰ For financial service providers that are obligated to verify the identity of account holders

4 ICRC, “The International Red Cross and Red Crescent Movement,” <https://www.icrc.org/en/who-we-are/movement>.

5 See, for example, “Head to Head: Biometrics and Aid”, *The New Humanitarian*, July 17, 2019, <https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid>; and Katja Lindskov Jacobsen, Kristin Bergtora Sandvik, and Sean Martin McDonald, “Humanitarian Experimentation,” ICRC, *Humanitarian Law & Policy*, November 28, 2017, <https://blogs.icrc.org/law-and-policy/2017/11/28/humanitarian-experimentation/>.

6 United Nations High Commissioner for Refugees, “Note on the Mandate of the High Commissioner for Refugees and His Office,” *Refworld*, October 2013, <https://www.refworld.org/docid/5268c9474.html>. Note: The ICRC also issues emergency travel documents, albeit very few by comparison.

7 See for example Chris Burt, “UNHCR Reaches 7.2M Biometric Records but Critics Express Concern,” *Biometric Update*, June 24, 2019, <https://www.biometricupdate.com/201906/unhcr-reaches-7-2m-biometric-records-but-critics-express-concern>.

8 The Engine Room and Oxfam, “Biometrics in the Humanitarian Sector,” March 2018: <https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf>.

9 Laura Gordon, “Risk and Humanitarian Cash Transfer Programming: Background Note for the High Level Panel on Humanitarian Cash Transfers,” *Overseas Development Institute*, May 2015, <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9727.pdf>.

10 See, for example, World Bank Group, “Guidelines for ID4D Diagnostics,” 2018, <http://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf>. Cash and other forms of direct financial disbursement are widely viewed as providing beneficiaries of humanitarian programs with more dignity and autonomy than food parcels and other disbursed goods, but donors are concerned that these programs are more susceptible to fraud and abuse.

and cash recipients, biometric data could offer a simple and straightforward way to meet multiple operational needs and legal obligations.¹¹

These are crucial issues for humanitarian staff, who want operations to be as efficient as possible, and to ensure that scarce humanitarian services and assistance are provided to intended recipients. There is also implicit pressure to use biometrics from donors, which increasingly demand “end-to-end auditability” (allowing the tracking of humanitarian funds from donor to recipient) and make funding contingent on anti-fraud and accountability processes. All of this has contributed to a tangible impetus for humanitarian organizations to use biometrics for beneficiary registration and aid distribution. And why not, if everyone else is doing it?

RISKS AND CONCERNS³

Concerns about the use of biometrics in the humanitarian sector are well known, but are often overlooked.¹² Biometric data are unique, immutable, and create a permanently identifiable record for individuals in vulnerable humanitarian contexts who may not want to be identifiable forever. The creation of a permanent biometric record underpins concern that this record could increase the risk of harm to the persons concerned in the event it was subsequently accessed by or provided to the regime or non-State actor they had fled.

Biometrics constitute particularly sensitive data¹³ due to the potential for reuse or misuse, as well as “function creep,” i.e., the possibility that biometrics may be used in a new way, separate from the original purpose and without the understanding or consent of the affected individuals. For example, biometrics could be shared with non-humanitarian organizations or governments for non-humanitarian purposes, such as security and migration control.¹⁴ This is particularly concerning when biometric identity management systems are developed during a crisis or

11 These assumptions also dovetail with the UN's Sustainable Development Agenda, which mandates the provision of legal identity to all and targets increased financial inclusion, tacitly encouraging States and the financial sector to predicate both on a biometric identity. See, for example, Sustainable Development Goal (SDG) target 16.9: “By 2030, provide legal identity for all, including birth registration: Promote just, peaceful and inclusive societies.” Financial inclusion is a target for eight of the seventeen SDGs. United Nations, Department of Economic and Social Affairs, Sustainable Development, “The 17 Goals,” <https://sdgs.un.org/goals>.

12 See, for example, Gus Hosein and Carly Nyst, “Aiding Surveillance,” *Privacy International*, October 2013, <https://privacyinternational.org/report/841/aiding-surveillance>. See also Katja Lindskov Jacobsen, “On Humanitarian Refugee Biometrics and New Forms of Intervention,” *Journal of Intervention and Statebuilding* 11, no. 4 (2017): 529–551, <https://doi.org/10.1080/17502977.2017.1347856>.

13 The General Data Protection Regulation (EU) 2016/679 (GDPR), for example, introduces a general prohibition against the processing of biometric data unless, inter alia, the data subject has given their “explicit consent” (something which is problematic in a humanitarian context, as discussed further below); the processing is subject to a specific law or legal agreement; the processing is necessary to protect the vital interests of data subjects who are physically or legally incapable of giving consent; or where the processing is necessary for reasons of public interest and subject to adequate measures to protect the interests and safeguard the fundamental rights of the data subject (Article 9). The recently adopted “Modernised CoE Convention 108+” on data protection broadly adopts the same approach to biometric data as the GDPR by classifying them as “sensitive data” and imposing core restrictions and conditions on their processing. The African Union Convention on Cybersecurity and Personal Data Protection also imposes restrictions on the processing of biometric data.

14 Affected populations have expressed serious concerns about the use of biometrics and potential access to the data by non-humanitarian organizations. See, for example, Aziz El Yaakoubi and Lisa Barrington, “Yemen's Houthis and WFP Dispute Aid Control as Millions Starve,” Reuters, June 4, 2019, <https://www.reuters.com/article/us-yemen-security-wfp/yemens-houthis-and-wfp-dispute-aid-control-as-millions-starve-idUSKCN1T51Y0>; “Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps,” *Radio Free Asia*, October 26, 2018, <https://www.rfa.org/english/news/myanmar/rohingya-refugees-protest-strike-11262018154627.html>; and “Over 2,500 Burundi Refugees in Congo Seek Shelter in Rwanda,” *Voice of Africa News*, March 8, 2018, <https://www.voanews.com/africa/over-2500-burundi-refugees-congo-seek-shelter-rwanda>.

emergency, where data could be used in ways that recipients of humanitarian assistance do not want, understand, or consent to. Humanitarian databases may, for example, be integrated or made interoperable with other social registries or national ID systems run by development or government partners. Technology may also advance to allow biometric profiles to be used to ascertain additional information about the data subject—for example regarding their health, ethnicity, or genetic makeup.

States have shown increasing interest in biometrics to monitor the movement of populations and identify security “threats.” In December 2017, the UN Security Council called for the enhanced use of biometric ID systems to identify terrorist suspects, mandating all UN Member States to “develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law.”¹⁵ Some humanitarian organizations have already come under pressure from States to disclose biometric data for non-humanitarian purposes, though these requests are generally not in the public domain. Organizations are also vulnerable to cyber-operations by State and non-State actors seeking unauthorized access to their data.¹⁶

Biometric data use was a central theme at the 33rd International Conference of the Red Cross and Red Crescent, held in December 2019.¹⁷ To safeguard the independence, neutrality, and trust in humanitarian organizations, the Conference adopted a landmark resolution on “restoring family links while respecting privacy.”¹⁸ Founded on the principle of purpose limitation, the resolution “urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement.”¹⁹

RATIONALIZING BIOMETRICS AT THE ICRC⁴

Prior to the adoption of its biometrics policy, the ICRC was already employing biometrics in limited use cases, for example in forensics and the restoration of family links, and by putting fingerprints on the travel documents it issues (but not into any database). In addition to using DNA profiling

15 UN Security Council Resolution 2396, adopted December 21, 2017 under Chapter VII of the UN Charter on “Foreign Terrorist Fighters.” As the UN Special Rapporteur for the Protection and Promotion of Human Rights While Countering Terrorism has stated, the biometrics mandate provided by the Security Council is “deeply concerning” because the Resolution does not contain any explicit reference to constitutional or legislative protections for privacy or data protection. See Fionnuala Ní Aoláin, “The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law,” *Just Security*, January 17, 2018, <https://www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/>.

16 Massimo Marelli, “Hacking Humanitarians: Moving towards a Humanitarian Cybersecurity Strategy,” ICRC, *Humanitarian Law & Policy*, January 16, 2020, <https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/>.

17 International Federation of Red Cross and Red Crescent Societies, 33rd International Conference, 2019, <https://rcrcconference.org/about/33rd-international-conference/>.

18 Reuniting families separated by conflict and disaster is a core activity of the International Red Cross and Red Crescent Movement globally. See “Restoring Family Links While Respecting Privacy, including as it Relates to Personal Data Protection” (33IC/19/R4), 33rd International Conference of the Red Cross and Red Crescent, December 9–12, 2019, https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-CLEAN_ADOPTED_en.pdf.

19 Ibid., Article 11.

to help identify human remains to determine the fate of the missing, the ICRC is exploring facial recognition technology to locate persons sought by family members following separation due to humanitarian emergencies.²⁰

This is part of a broader ICRC strategy to transform and adapt its humanitarian response by seizing the opportunities that new technologies offer its operations and beneficiaries. Managing the attendant risks is central to this digital transformation agenda.²¹ Early in 2018, following significant interest in expanding biometric data use, the ICRC Directorate requested an assessment of the operational, ethical, and reputational risks involved, as well as an institution-wide policy that would facilitate both innovation and data protection.

ICRC developed the policy over an eighteen-month period that included extensive research, analysis, consultation, and reflection. ICRC reviewed all scenarios in which the ICRC processed or considered the use of biometrics, evaluated the “legitimate basis” and specific purposes for the processing, and identified organizational, technical, and legal safeguards. Although the ICRC is not bound by national or regional data-protection law, it has adopted similar rules that require it to identify a legitimate basis (equivalent to a legal basis) for all of its data-processing activities.²²

In some cases, ICRC’s rationale for biometric data use was straightforward: for instance, when used with specific objectives associated with its international mandate and where particular objectives cannot be realized without using biometrics. Examples include using DNA to determine the fate or whereabouts of the missing, or using facial recognition to match missing and sought persons in its work on restoring family links.²³ In these cases, the ICRC processes the biometric data as a matter of “public interest.”²⁴ Subject to appropriate safeguards, biometric data processing provides the ICRC with tools that greatly enhance its capacity to implement its mandate with respect to persons separated or missing in humanitarian emergencies.

Other cases are much more challenging: for example, when the potential use case involves biometrics for beneficiary management and aid distribution, where requiring the identification of individuals may not be viewed as an integral part of an ICRC mandate-based activity. Because the purpose is primarily efficiency, and aid can be (and long has been) distributed without the need for biometrics, the ICRC determined that the “legitimate interest” of using a biometric identity-management system did not outweigh the potential concerns over rights and freedoms. This balancing test is typical of data-protection laws (e.g., as in GDPR), whenever a data controller relies on their own interests as a basis for processing.²⁵

20 See “Rewards and Risks in Humanitarian AI: An Example,” ICRC, *Inspired*, September 6, 2019, <https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence/>.

21 In addition to “doing no harm,” ICRC maintains principles of impartiality, neutrality, and independence. The protection of personal data that could be misused or whose disclosure could put its beneficiaries at risk is an integral means of ensuring these principles are upheld. See ICRC, “The Fundamental Principles of the International Red Cross and Red Crescent Movement,” https://www.icrc.org/sites/default/files/topic/file_plus_list/4046-the_fundamental_principles_of_the_international_red_cross_and_red_crescent_movement.pdf.

22 See ICRC, “Rules on Personal Data Protection,” (“ICRC Rules”), <https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection>. The rules were adopted by the Directorate of the ICRC on February 24, 2015 (updated on November 10, 2015), and updated and adopted by the ICRC Assembly on December 19, 2019.

23 ICRC, Restoring Family Links, <https://familylinks.icrc.org/en/Pages/home.aspx>.

24 ICRC Rules, Article 1.

25 ICRC Rules, Article 1; GDPR, Article 6.

After careful consideration, ICRC concluded that it was possible to leverage the efficiency and effectiveness gains of biometric authentication, as well as end-to-end accountability in its aid distributions, while also minimizing the risks to its beneficiaries. This balance rests on using biometric data in beneficiary registration and verification, and limiting the processing to a token-based system. In practice, this means that beneficiaries could be issued a card on which their biometric data is securely stored, but that the ICRC will not collect, retain, or further process their biometric data (and therefore not establish a biometric database).

The token/card could be used to verify beneficiaries during aid distributions to ensure that the aid reaches those individuals for whom it has been earmarked, but no other use will be possible. If the beneficiary wants to withdraw or delete their biometric data, they may return or destroy the card. If authorities seek to compel humanitarian organizations in a particular country to hand over the biometric data of beneficiaries, the ICRC will not face such pressure because it will not have the data.

KEY FEATURES OF THE POLICY

Adopted by the ICRC Assembly in August 2019, the ICRC Biometrics Policy sets forth staff and program roles and responsibilities,²⁶ the legitimate basis for processing biometric data by the ICRC,²⁷ the specific purposes and use cases for which the use of biometrics is authorized,²⁸ and the types of biometric data that may be processed by the ICRC.²⁹ Specifically, it allows the ICRC to:

- include the fingerprints of the holder on travel documents issued by the ICRC to persons who have no valid identity papers, enabling them to return to their country of origin or habitual residence or to go to a country which is willing to receive them;
- use biometric identification systems to restrict access to strictly confidential information and/or mission-critical resources such as servers and control rooms in ICRC premises;
- use fingerprints, facial scans, and DNA to identify human remains recovered from disaster or conflict zones or in connection with other situations of violence;
- use digitized photographs for the purposes of tracing and clarifying the fate of separated or missing persons;
- use biometric data to ascertain the identity or fate of specific individuals in the course of investigations related to the abduction of, or attacks upon, ICRC staff members;
- on a case-by-case basis, where it has been determined that it is in the best interest of the persons concerned, collect biological reference samples for the purposes of DNA profiling to facilitate family reunification or to determine the fate of a missing person; and
- use biometrics to provide beneficiaries with a token-based verification credential such as a card that can be used to verify their receipt of those services, where the token is held solely by the Data Subject.

²⁶ ICRC Biometrics Policy, Article 4.

²⁷ Ibid., Article 5.

²⁸ Ibid., Article 6.

²⁹ Ibid., Article 7.

There are additional caveats:¹

- The use of fingerprints for travel documents remains limited to ink prints on hard-copy documents (with no further biometric processing by the ICRC permitted).²
- Delegations may not use biometrics for routine premises control (only specific assets that require a high level of security and where profiling is limited to staff authorized to access them).
- DNA profiling for family reunion purposes is strictly limited to cases where proof that two persons are actually related is required under national law or policy.

The Policy also expressly rules out the creation of biometric databases with respect to the authorized use cases. Finally, where ICRC programs or delegations wish to process biometric data pursuant to an authorized use case, they must first conduct a data-protection impact assessment and ensure that detailed data protection by design and by default requirements are implemented as the process or system is developed.³⁰³

The Biometrics Policy also addresses some other common data-protection challenges, including “consent,” which humanitarian organizations have traditionally sought from the people who use their services or receive assistance. In some contexts, like medical treatment, these processes have been quite robust. In others, however, people have routinely signed “consent forms” or provided a thumbprint in lieu of a signature (e.g., for those unable to write; as part of its biometrics review, the ICRC is also putting an end to this practice). “Informed consent” in data processing is subject to high standards: the ICRC Rules on Personal Data Protection require “freely given, specific, informed indication of his or her wishes by which a Data Subject signals agreement to the Processing of Personal Data relating to him or her.”³¹⁴

While the ICRC is firmly committed to transparency, it does not believe that consent provides a legally valid basis for data processing in many emergency situations. Consent to data processing cannot be regarded as valid if the individual has no real choice: for example, where the provision of aid is effectively dependent on the provision of personal information, and consent is therefore unlikely to be “freely given.” In addition, power imbalances may imply no real “choice,” and individuals may be induced to accept what is proposed by a humanitarian organization. Where biometrics are concerned, it is extremely difficult to ensure that consent is genuinely “informed,” since affected populations may not be able to fully comprehend the technology, information flows, risks, or benefits that underpin biometric data processing.⁵

The Biometrics Policy requires that the ICRC explain the basis and purpose of data processing to its beneficiaries, including any data-sharing arrangements, regardless of the basis for the processing.³² The ICRC also seeks to ensure that beneficiaries have the opportunity to ask questions and object if they wish, particularly where data may be shared with third parties.³³ If people do not want to provide their biometric or other personal data, or share their data with

³⁰ Ibid., Articles 10 and 11.

³¹ ICRC Rules, Definitions: “Consent.”

³² ICRC Biometrics Policy, Article 18. This is in line with the ICRC Rules on Personal Data Protection.

³³ Ibid., Article 18.4.

partners, the ICRC will respect their wishes.³⁴ The ICRC will only use biometric data where it enhances the capacity of the organization to implement its humanitarian mandate.³⁵ 1

Finally, under no circumstances will the ICRC share biometric data with third parties, including authorities, that may use them for non-humanitarian purposes.³⁶ Even where exclusively humanitarian grounds for sharing biometric data can be identified, strict conditions must be satisfied before ICRC will transfer any data.³⁷ 2

The ICRC will review the Biometrics Policy at least every three years,³⁸ including the decision not to establish biometric databases for the purposes of identity management. ICRC will review developments around the availability, security, cost, effectiveness, and impact of biometric technology, and may amend the Policy to widen the scope for using biometrics, or to introduce new safeguards. 3

LESSONS LEARNED 4

During its deliberations, the ICRC considered the option of not adopting a biometrics policy and leaving decisions about how and when to use these data to programs, operations, and delegations in the field. This option was rejected as “high risk on the basis that it could undermine, *inter alia*, the rights of the ICRC’s beneficiaries, the ‘do no harm’ principle, and ICRC’s reputation.” While the internal organizational debates have been challenging, the Policy has provided much needed clarity and operating procedures for staff who were struggling to balance the perceived benefits and risks of specific uses. 5

ICRC consulted internal staff and external stakeholders in order to answer questions around operational needs, data-protection requirements, technology options, ethics, and risk appetite. Case-by-case assessment of the existing and possible use cases was fundamental in shaping the ICRC Biometrics Policy. However, ICRC faced many challenges because it was already using biometrics, and the new Policy could have led to changes in practice or prohibitions against certain processing options or operations. Finally, the ICRC Biometrics Policy benefited from considerable dialogue and investment in innovative compromises such as the token-based solution, which might not have been achieved through a less coherent or constructive exercise. As biometric data use-case law and data-protection enforcement actions continue to expand, the need for humanitarian organizations to develop proactive policies only becomes more important. 6

³⁴ Ibid., Articles 19 and 20.

³⁵ Ibid., Article 6.1.

³⁶ Ibid., Article 14.

³⁷ Ibid., Article 15.

³⁸ Ibid., Article 21.

Policing Uses of Live Facial Recognition in the United Kingdom¹

Peter Fussey (University of Essex)²
Daragh Murray (University of Essex)

BACKGROUND TO THE USE OF FACIAL RECOGNITION IN THE UK³

London has a long history of trialing advanced surveillance technology. Police agencies first installed closed-circuit television (CCTV) cameras in the city in 1953, and until recently London likely had more CCTV cameras per person than any country in the world.¹ The city deployed one of the world's first automatic license plate recognition (ALPR) systems in the mid-1990s, and has since introduced crowd-modeling video analytics to survey its mass transit systems.² London was also one of the first cities in the world to trial facial recognition (FR) in the east of the city during the late 1990s, although technological limitations at the time led to its abandonment.³

1 Pete Fussey, "Beyond Liberty, Beyond Security: The Politics of Public Surveillance," *British Politics* 3, no. 1 (April 2008): 120–135. See also Jess Young, "A History of CCRV Surveillance in Britain," SWNS, January 22, 2018, <https://stories.swns.com/news/history-cctv-surveillance-britain-93449/>. London remains the most CCTV-heavy city outside of China.

2 Pete Fussey, "Observing Potentiality in the Global City: Surveillance and Counterterrorism in London," *International Criminal Justice Review* 17, no. 3 (September 1, 2007): 171–192.

3 Pete Fussey, "Eastern Promise? East London Transformations and the State of Surveillance," *Information Polity*, 17, no. 1 (January 2012): 21–34.

With rapid advancements in FR technology, the Metropolitan Police Service (MPS) conducted a series of ten live facial recognition (LFR) test deployments between 2016 and 2019, moving to operational deployments in early 2020.⁴ South Wales Police have also been using LFR since 2017, mostly at large concerts, festivals, and sporting events.⁵ Both constabularies deploy LFR by installing temporary cameras at a fixed geographic location⁶ for a fixed time period.⁷ Police generally mount the cameras on an LFR van with a control center used to monitor the live LFR feeds and to communicate with officers on the ground. LFR cameras scan the faces of all individuals passing through their field of vision, and then officers check the resultant biometric profiles against a watch list containing persons of interest. To date, police have only deployed LFR technology in this standalone manner, and have not, for example, integrated it into existing infrastructure, such as CCTV networks.⁸

Police use of LFR has resulted in significant controversy, with a number of human rights and civil society organizations leading opposition against LFR deployments. Many of these organizations have initiated advocacy campaigns calling for either a moratorium on the use of LFR,⁹ or an outright prohibition.¹⁰ South Wales Police's use of LFR is currently subject to legal challenge, and an initial hearing before the Court of Appeal took place in June 2020.¹¹

In order to examine issues relating to operational effectiveness and human rights compliance, the MPS invited the authors to provide an independent academic report on the last six LFR test deployments.¹² We conducted ethnographic observations from beginning to end of each deployment, of pre-deployment police briefings and post-deployment debriefings, and of a range of other planning meetings. We also held interviews with key stakeholders and analyzed large quantities of MPS internal documents. In this piece, we draw on this research to explore three key themes relating to the regulatory regime: 1) the legal requirement for an authorizing law for LFR; 2) the inability and failure of existing institutions and laws to meaningfully restrict this technology; and 3) the operational considerations unique to LFR. Our focus is on working toward human rights compliance. A key element not addressed in this piece is the "necessity" of police LFR deployments. However, this consideration only comes into play if an appropriate legal basis exists.

4 Having moved out of the "test" phase, the MPS now has authority to deploy LFR on the basis of operational intelligence. For further information, see Metropolitan Police, "Live Facial Recognition," n.d., <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/>.

5 For more information, see South Wales Police, "Facial Recognition Helps South Wales Police Become Smarter, Creating a Safer and Connected Community," n.d., <http://afr.south-wales.police.uk>. The list of deployments is available at <https://afr.south-wales.police.uk/wp-content/uploads/2020/04/All-Deployments.pdf>.

6 A "fixed location" might be a city square, the entrance to an underground tube station, or a football match, for example.

7 This is typically a number of hours; to date, no deployments have lasted longer than a day.

8 Although this is becoming increasingly technologically feasible, it is unlikely that these more advanced LFR deployments will occur in the short term.

9 See, for example, Carly Kind, "Biometrics and Facial Recognition Technology—Where Next?" Ada Lovelace Institute, July 2, 2019, <https://www.adalovelaceinstitute.org/biometrics-and-facial-recognition-technology-where-next/>.

10 See, for example, Liberty, Resist Facial Recognition, <https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/>; and Big Brother Watch, Stop Facial Recognition, <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>.

11 The complaint was brought by Ed Bridges, who believes he was subject to facial recognition processing at a peaceful anti-arms trade protest, and while Christmas shopping. See Liberty, "Liberty Client Takes on Police in Ground-Breaking Facial Recognition Challenge—Hearing Opens Today, May 21, 2019," <https://www.libertyhumanrights.org.uk/issue/liberty-client-takes-on-police-in-ground-breaking-facial-recognition-challenge-hearing-opens-today/>.

12 Peter Fussey and Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology," University of Essex Human Rights Centre, section 2.1.1, July 9, 2019, <http://repository.essex.ac.uk/24946/>.

Police LFR deployments directly engage / interfere with several distinct human rights protections.¹ The right to privacy of all individuals passing through a camera's field of vision (and thus subject to biometric processing) is directly engaged. Additional, discrete right-to-privacy issues are raised by any retention or analysis of the resultant footage.¹³ The use of LFR may also engage discrimination laws as a result of the technology's biases.¹⁴ Importantly, the deployment of LFR technology may generate a chilling effect, whereby individuals refrain from lawfully exercising their democratic rights due to a fear of the consequences that may follow.¹⁵ This may harm a number of rights, including the right to freedom of expression, the right to freedom of assembly and association, and the right to freedom of religion.¹⁶

Significantly, the UK's Human Rights Act 1998 (implementing the European Convention on Human Rights¹⁷), requires that any interference with a right be "in accordance with the law." As such, any measure interfering with human rights protections must have a legal basis, and that legal basis must be of sufficient quality to protect against arbitrary rights interferences. Key in this regard is the foreseeability of the law.¹⁸ If a measure fails to satisfy the "in accordance with the law" requirement, it is unlawful in and of itself.

THE COMMON LAW AS A LEGAL BASIS FOR LIVE FACIAL RECOGNITION³

United Kingdom common law establishes the core common law principles for police: protecting life and property, preserving order, preventing the commission of offenses, and bringing offenders to justice.¹⁹ Although no legislation exists that explicitly authorizes police use of LFR, the government has claimed that these common-law powers provide sufficient implicit legal authorization to satisfy the "in accordance with the law" test.

In *Bridges v. South Wales Police*, the UK High Court agreed with the Government,²⁰ indicating that the common law establishes sufficient legal basis for LFR.²¹ This judgment is currently subject to appeal, and this finding is a key point of contention.

13 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 59.

14 For further discussion on indirect discrimination, see *D.H. and Others v. the Czech Republic*, Judgment ECtHR, App. No. 57325/00, November 13, 2007, para. 184.

15 The precise contours of any chilling effect are contested, but research points to its existence. See Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31, no. 1 (2016): 117; see also Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly* 93, no. 2 (2016): 296–311; for a general discussion, see Daragh Murray and Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data," *Israel Law Review* 52, no. 1 (March 2019): 31–60. For a discussion of the chilling effect as it applies to journalists, see *Centro Europa 7 S.R.L. and Di Stefano v. Italy*, Judgment, European Court of Human Rights, App. No. 38433/09, June 7, 2012, para. 129.

16 For a more in-depth discussion of potential human rights harms, see Fussey and Murray, "Independent Report," section 2.1.2, <http://repository.essex.ac.uk/24946/>.

17 See, e.g., *Shimovolos v. Russia*, Judgment, ECtHR, App. No. 30194/09, June 21, 2011, para. 67.

18 *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, January 24, 2019, para. 94.

19 See, for example, Metropolitan Police, "Live Facial Recognition, (LFR) MPS Legal Mandate," p. 5, July 23, 2018, <https://www.statewatch.org/media/documents/news/2018/dec/uk-live-facial-recognition-lfr-mps-legal-mandate.pdf>.

20 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 78: "For these reasons, we consider the police's common law powers to be 'amply sufficient' in relation to the use of AFR Locate. The police do not need new express statutory powers for this purpose." ("AFR Locate" is South Wales Police's nomenclature for LFR.)

21 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 78.

At the heart of the matter is the fact that police powers under the common law are expressed in broad terms. The common law is inappropriately vague and, for example, does not delimit the circumstances in which a particular measure may be deployed, such that those circumstances are foreseeable, thereby protecting against arbitrary rights interference. Relying on the common law to provide a legal basis for LFR therefore arguably fails to satisfy the “in accordance with the law” requirement established under human rights law, and presents a clear risk of arbitrariness.²²

A key reason for the High Court’s conclusion that the common law was a sufficient legal basis for LFR, and that new statutory powers were not required, was the classification of LFR as a nonintrusive means of obtaining information,²³ and as “no more intrusive than the use of CCTV in the streets.”²⁴ This is clearly contentious: it appears inconsistent with common understandings of the surveillance capacity inherent in LFR, and has been challenged by a number of key figures in the UK. It also appears inconsistent with the High Court’s own finding that—as a form of biometric processing—LFR engaged the right to privacy of all individuals passing through an LFR camera’s field of vision.²⁵

Concerns regarding the arbitrary exercise of powers mean that reliance on the common law to provide the legal basis for the use of LFR is likely to be incompatible with the UK’s obligations under the Human Rights Act or European Convention on Human Rights. The Bridges line of cases will provide further guidance in this regard. However, irrespective of the outcomes of these cases, establishing an explicit legal and regulatory basis for the use of LFR would provide much needed clarity, both for the public and for the police.

OTHER LAWS, LEGISLATIONS, AND AGENCIES THAT APPLY TO LFR

Police documentation and political debate have consistently referred to the oversight roles of the multiple data-protection and surveillance-related authorities in the UK.²⁶ These include the UK’s data-protection authority, the Information Commissioner’s Office (ICO); the Surveillance Camera Commissioner; the Biometrics Commissioner; and the Investigatory Powers Commissioner’s Office. While these agencies have contributed to the debate, each body is narrowly relevant to a specific aspect of LFR and, critically, they do not have explicit authorization to limit LFR deployments. Indeed, while many of these regulatory bodies are heralded as a safeguard to promote appropriate use, their mandates do not provide meaningful oversight. This is explained in the following table:

22 This concern is equally applicable vis-à-vis the regulation of LFR deployments. The human rights law tests regarding clarity, foreseeability, and protection against arbitrariness are equally applicable in this regard. This conclusion is supported by relevant case law. See, for example, *S and Marper v. United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, December 4, 2008, para. 99.

23 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 74.

24 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 75.

25 This finding distinguishes LFR as more invasive than CCTV. See *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, paras. 59, 62.

26 As noted above, these considerations are irrelevant if the “in accordance with the law” requirement is not satisfied.

Authority	Role	Application to LFR
The Information Commissioner's Office (ICO)	Oversees issues relating to data protection in the UK, particularly the Data Protection Act 2018 and the General Data Protection Regulation. ²⁷ In 2017, they published "In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information," which provided best practices for automated recognition technologies. ²⁸	Although important, data protection law cannot adequately address the broad range of potential human rights harms brought about by police LFR deployments. It does not, for example, fully address issues relating to whether the use of LFR is necessary or proportionate. As such, the impact of the ICO on the overall LFR debate is relatively limited.
The Surveillance Camera Commissioner	Established by the Protection of Freedoms Act 2012 to oversee the use of closed-circuit television systems (CCTV). ²⁹	While they are primarily focused on CCTV systems, and LFR is implemented through standalone video systems, they have published guidance on police use of LFR. ³⁰
The Biometrics Commissioner	Established by the Protection of Freedoms Act 2012 to oversee retention and use of biometric information. ³¹	The Biometrics Commissioner's role is restricted in statute to fingerprints and DNA data, and so does not extend to LFR. The Commissioner has published several statements questioning the use of LFR and has said that "we need proper governance of new biometric technologies such as LFR through legislation." ³²
The Investigatory Powers Commissioner's Office	Established under the Investigatory Powers Act 2016, has authority to oversee covert police deployments. ³³	As currently deployed, the principal uses of LFR by police in the UK are not classified as covert. This may change going forward.

27 See, further, the Information Commissioner's Office (ICO), <https://ico.org.uk/about-the-ico/>.

28 ICO, "In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information," Version 1.2, June 9, 2017, <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>.

29 Protection of Freedoms Act ref. See, further, the Surveillance Camera Commissioner, <https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about>.

30 See, for example, the Surveillance Camera Commissioner's Code of Practice, June 2013, <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>; and "The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems," Section 33 Protection of Freedoms Act 2012, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

31 Protection of Freedoms Act ref. See, further, Office of the Biometrics Commissioner, <https://www.gov.uk/government/organisations/biometrics-commissioner/about>.

32 See, for example, GOV.UK, "Automated Facial Recognition," September 10, 2019, <https://www.gov.uk/government/news/automated-facial-recognition>, <https://www.gov.uk/government/news/biometrics-commissioner-on-the-police-use-of-live-facial-recognition>.

33 Investigatory Powers Act 2016, <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>.

As it stands, police use of LFR in the UK is not subject to adequate oversight or meaningful regulation. This must urgently be addressed.¹

ISSUES ARISING IN THE CONTEXT OF POLICE LIVE FACIAL RECOGNITION DEPLOYMENTS²

This section examines a number of issues arising in the context of LFR deployments, including watch lists, the “presumption to intervene” and associated deficits in effective human oversight, how accuracy is determined, and potential discrimination. These operational elements illustrate the uncertainty associated with LFR deployments, contesting police claims of utility, and highlight problems arising from the absence of appropriate regulation.³

*Operational Considerations*⁴

Measuring LFR performance is complex and includes both partial and instrumental use of statistics. Some technical evaluations compare the number of false matches to an estimate of the total number of individuals passing through an LFR camera’s field of vision during a given deployment. These numbers are widely cited by supporters of LFR, yet they offer only a tiny ratio of numbers of faces scanned to those correctly or incorrectly matched.³⁴ A variation of this approach was adopted by the MPS in a recently published evaluation of their LFR trial deployments,³⁵ leading to widely publicized claims that the technology was “70% effective.”³⁶ However, such claims often conflate two different forms of data, merging “blue list” data (where volunteers are sent past the cameras to measure their effectiveness—the measure used to support the claim of 70 percent effectiveness) and live data (camera performance when there is no certainty about whether suspects will walk past the cameras).⁵

Another shortcoming of this methodology is the way it de-emphasizes the impact of LFR on those flagged by the technology by contextualizing their experience against larger quantities of data that are arguably less relevant. This makes this measure less suitable for understanding the individual rights-based interferences brought by LFR. Other measures of LFR performance compare how often a human operator discards a computer-suggested alert.³⁷ One challenge of this approach is the potential for readers to conflate human and computer decision-making: a human might decide the LFR system is wrong, regardless of the veracity of the computational decision.⁶

³⁴ See comments by Baroness Williams of Trafford regarding “a one in 4,500 chance of triggering a false alert,” House of Lords, January 27, 2020, <https://www.theyworkforyou.com/lords/?id=2020-01-27a.1300.2&p=12902>.

³⁵ National Physical Laboratory and Metropolitan Police Service, “Metropolitan Police Service Live Facial Recognition Trials,” February 2020, <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf>.

³⁶ Vikram Dodd, “Met Police to Begin Using Live Facial Recognition Cameras in London,” *Guardian*, January 24, 2020, <https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras>.

³⁷ Bethan Davies, Martin Innes, and Andrew Dawson, *An Evaluation of South Wales Police’s Use of Automated Facial Recognition* (Cardiff: Universities’ Police Science Institute, Crime and Security Research Institute, Cardiff University, 2018).

We designed our independent academic review of the MPS system to address the above challenges, focusing on human rights considerations and protection against arbitrary rights interferences. The research used the same statistics as the MPS study above,³⁸ and asked two straightforward questions to determine accuracy and examine the role of human oversight:

- a. When an LFR system matches someone to the watch list, how often is it verifiably correct?³⁹
- b. To what extent do human adjudicators consider LFR matches to be credible? To understand if a computer match is correct, it needs to be tested against something—in this case, an identity check of the suspect.

For (a), our research found that out of forty-two computer-generated LFR matches, eight were verifiably correct (19.05 percent). For (b), human adjudicators judged twenty-six out of forty-two matches were sufficiently credible to apprehend the matched individual (61.91 percent), meaning that humans overwhelmingly overestimated the credibility of the system. Four of these matched individuals were lost in the crowd. The remaining fourteen were incorrectly matched by the LFR system.

Two conclusions can be drawn from this. First, there is a “presumption to intervene” on behalf of human operators assessing the credibility of LFR matches. Second, this tendency of deference to the algorithm exists despite the computer being either incorrect or not verifiably correct in a large majority of cases.

These conclusions hold relevance for considerations over the form of human adjudication taking place around LFR systems. Policy emphasizes the importance of “the human in the loop” as a safeguard against algorithmic-induced harms. That human adjudication takes place is not in question, however. The issue at stake is the form it takes, and the degree of critical human scrutiny applied. Moreover, a presumption to intervene suggests LFR frames and structures suspicion ahead of human engagement with the technology.

A final question is whether LFR is discriminatory. UK police forces have made repeated claims that LFR technology is nondiscriminatory in terms of racial characteristics.⁴⁰ However, this is a complex issue and covers both the capability of the technology in identifying faces from a range of ethnic groups and the composition of databases of suspects (watch lists). It is difficult for law enforcement agencies to undertake an analysis of sufficient scope to support definitive conclusions. For example, the US National Institute of Standards and Technology (NIST) reviewed 189 facial recognition algorithms and revealed marked “demographic differentials” in the performance of facial recognition algorithms across different ethnicities.⁴¹ Accordingly, claims made in the technical evaluation of the MPS LFR scheme that “differences in FR algorithm performance due to ethnicity are not statistically significant”⁴² may arise simply because the total number of matches themselves are not statistically significant.

38 Sup. 35.

39 In other words, could it be definitively concluded that the individual identified by LFR matched the individual on the watch list, such as by means of a subsequent identity check?

40 See, for example, public statements by Metropolitan Police Commissioner Dame Cressida Dick, RUSI Annual Security Lecture, London, February 24, 2020. “The tech we are deploying is proven not to have an ethnic bias.” Available here: <https://rusi.org/event/rusi-annual-security-lecture>.

41 Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,” NIST, December 2019, <https://doi.org/10.6028/NIST.IR.8280>.

42 National Physical Laboratory and Metropolitan Police Service, “Metropolitan Police Service Live Facial Recognition Trials,” p.4.

According to the MPS statistics, twenty-eight people were engaged by a police officer after being matched by LFR systems across their ten test deployments. We contend that it is impossible to make robust and definitive conclusions over demographic disparities from such small numbers. Concerns over this issue have been most recently articulated in March 2020 in calls by Great Britain's Equality and Human Rights Commission to suspend the use of facial recognition in England and Wales until its impact has been independently scrutinized.⁴³

CONCLUSION²

This piece highlights three key concerns. First, the legal basis underpinning LFR is inappropriately vague, negatively affecting foreseeability, and arguably failing to meet the "in accordance with the law" test established by human rights law. Second, although a number of UK regulatory bodies engage in this area, there is no dedicated body with authority to limit or effectively oversee LFR deployments. Third, operational realities contest police claims of LFR's utility, the effectiveness of human oversight, and discriminatory outcomes. These highlight the practical consequences and harms arising in the absence of appropriate legal or regulatory frameworks.

43 Equality and Human Rights Commission, "Facial Recognition Technology and Predictive Policing Algorithms Out-pacing the Law," March 12, 2020, <https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law>.

A Taxonomy of Legislative Approaches to Face Recognition in the United States¹

Jameson Spivack (Georgetown Center on Privacy and Technology)²
Clare Garvie (Georgetown Center on Privacy and Technology)

INTRODUCTION: POLICE FACE RECOGNITION IN THE UNITED STATES³

On December 25, 2015, Florida resident Willie Allen Lynch was arrested for selling fifty dollars' worth of crack cocaine to two undercover Jacksonville sheriffs three months earlier. The only thing tying Mr. Lynch to the crime was a face recognition search comparing photographs the officers had taken of the drug sale to the county's mugshot database. The search returned five possible matches—Mr. Lynch and four other suspects. Mr. Lynch and his defense attorney were given no information about the use of face recognition: its accuracy, potential biases, or even a list of the other possible suspects. Despite this, Mr. Lynch, who maintains his innocence, was sentenced to eight years in prison.⁴

¹ See *Lynch v. State*, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018). For an overview of how face recognition was used in the case, see *Lynch v. State*, No. SC2019-0298 (Fla. Sup. Ct. 2019), *Amici Curiae Brief in Support of Petitioner*, available at https://www.aclu.org/sites/default/files/field_document/florida_face_recognition_amici_brief.pdf. The lower court's decision was affirmed on appeal, and the State Supreme Court determined it did not have jurisdiction to hear the case. *Lynch v. State*, SC2019-0298 (Fla. Sup. Ct. 2019).

Police use of face recognition is pervasive, affects most Americans, and, until very recently, has persisted under a widespread lack of transparency, oversight, and rules governing its use.² Police departments across the United States have deployed face recognition technology in thousands of criminal investigations since as early as 2001.³ At least one agency has also used face recognition to identify protesters,⁴ and by 2016, one quarter of the nearly eighteen thousand agencies across the country had access to a face recognition system.⁵ Because thirty-one states allow police searches of DMV databases, more than half of all American adults can be identified through police face recognition simply by having a driver's license.⁶ Many police departments have also used Clearview AI's face recognition service, which has amassed a database of an additional three billion images scraped from Facebook, Instagram, Twitter, Venmo, YouTube, and elsewhere.⁷

In 2016, the Government Accountability Office (GAO) published an extensive report on the use of face recognition by the FBI.⁸ It made recommendations to increase transparency, enhance privacy protections, and better test the accuracy of their systems to guard against misidentification. This and many other reports have highlighted unique risks posed by police face recognition use:

- **Face recognition poses a threat to privacy.** Under the Fourth Amendment of the US Constitution, the right to privacy extends beyond the home, protecting “reasonable expectations of privacy” in some public settings and activities.⁹ Face recognition gives police the power to conduct identity-based surveillance and the ability to scan and identify groups of people in secret, as well as to track someone's whereabouts through a network of security cameras. Without a warrant, this power may violate the Fourth Amendment, interpreted in the Supreme Court's 2018 decision in *Carpenter v. United States* as including a right to privacy in our movements across time and space.¹⁰ The enrollment of most American adults into biometric databases used in criminal investigations represents an unprecedented expansion of law enforcement access to personal data, to which the American public did not consent.¹¹

2 For an overview of the state of face recognition and laws governing its use, see Clare Garvie, Alvaro M. Bedoya, and Jonathan Frankle, “The Perpetual Line-Up: Unregulated Face Recognition in America,” Georgetown Law Center on Privacy & Technology, (October 18, 2016): 25, 35, <https://www.perpetuallineup.org/report>.

3 See Pinellas County Sheriff's Office, *Florida's Facial Recognition Network* (Mar. 26, 2014), available at <https://drive.google.com/file/d/0B-MxWJP0ZmePX1QwTjltQkdVX0U/view?usp=sharing> (indicating 2001 as the start date for the Sheriff Office's system).

4 Geofeedia, *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots* (obtained by ACLU Northern California Oct. 11, 2016), available at https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

5 See *supra* note 2, at 25. This is a conservative estimate—the actual number is likely much higher. Prior to being terminated by the Attorney General's Office, all law enforcement agencies in the country were able to request searches of the Vermont driver's license face recognition system. See *ACLU Demands Immediate End to DMV Facial Recognition Program*, ACLU-VT (May 24, 2017), www.acluvt.org/en/press-releases/aclu-demands-immediate-end-dmv-facial-recognition-program.

6 See *Statement of Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law before the U.S. House of Representatives Committee on Oversight and Reform* (May 22, 2019), 5, available at <https://docs.house.gov/meetings/GO/G000/20190522/109521/HHRG-116-G000-Wstate-GarvieC-20190522.pdf>.

7 See 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>. Former Center technologist Jonathan Frankle cautioned against just such a tool in 2016. See Jonathan Frankle, “How Russia's New Facial Recognition App Could End Anonymity,” *Atlantic*, May 23, 2016, <https://www.theatlantic.com/technology/archive/2016/05/find-face/483962/>.

8 Government Accountability Office (GAO), “Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,” May 2016, <https://www.gao.gov/assets/680/677098.pdf>.

9 U.S. Const. Amend. IV; *Katz v. United States*, 389 U.S. 347 (1967).

10 *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

11 See *supra* note 6, at 5–7.

- **Face recognition risks having a chilling effect on free speech.** The First Amendment of the US Constitution protects the right to free speech, assembly, and association.¹² As law enforcement agencies themselves have cautioned, face recognition surveillance has the potential to “make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition”—chilling our ability to participate in constitutionally protected activities.¹³ 1
 - **Searches may lead to misidentifications.** While the algorithms behind face recognition have improved significantly since 2001, misidentification is still a major issue. Low-quality images, edited photos, and unreliable inputs such as forensic sketches and “celebrity lookalikes” increase the odds that the wrong person will be investigated, arrested, and charged with a crime they did not commit.¹⁴ 2
 - **Face recognition may have a disparate impact on communities of color.** Communities of color are disproportionately enrolled in face recognition databases and targeted by surveillance.¹⁵ In San Diego, for example, police have used face recognition technology and license-plate readers up to two and a half times more on people of color than expected by population statistics.¹⁶ The technology performs less accurately on people of color, meaning the risks of the face recognition police use, and the mistakes it may make, will not be distributed equally. 3
 - **The failure to disclose a face recognition search may deprive a defendant of due process.** The risks of misidentification and bias are not mitigated by a fair, transparent court process. Face recognition searches produce evidence that speaks directly to a defendant’s guilt or innocence. Per the constitutional right to due process and the Supreme Court’s decision in *Brady v. Maryland*, evidence must be turned over to the defense.¹⁷ Yet as in Mr. Lynch’s case, and indeed the vast majority of cases involving a face recognition search, this information is not disclosed.¹⁸ 4
- In response to growing concern over the risks that the use of unregulated police face recognition poses to our civil rights and liberties, legislators have begun introducing—and passing—face recognition bans, moratoria, and regulatory bills.¹⁹ 5

¹² U.S. Const. Amend. I.

¹³ International Justice and Public Safety Network (Nlets), “Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field,” June 30, 2011, 2, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

¹⁴ For a discussion of how face recognition is used in practice and its associated risks, see Clare Garvie, “Garbage In, Garbage Out: Face Recognition on Flawed Data,” Georgetown Law Center on Privacy & Technology, May 16, 2019, <https://www.flawedfacedata.com>.

¹⁵ See *supra* note 2 at 56 (describing disproportionately high arrest rates of black Americans); see Grother, Ngan, & Hanoaka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Nat’l Institute of Standards and Technology (NIST) (Dec. 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> (“We found empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms that we evaluated.”).

¹⁶ See, e.g., Automated Regional Justice Information System, *San Diego’s Privacy Policy Development: Efforts & Lessons Learned*, 11, available at <https://drive.google.com/file/d/1ZR2jjiLcBMUKnHTRk1ZC248NbFUqNRww/view?usp=sharing> (indicating that black Americans were 1.5–2.5 times more likely to be the targets of police use of licence-plate readers and face recognition technology).

¹⁷ *Brady v. Maryland*, 373 U.S. 83, 87 (1963) (holding that the suppression of evidence that is material to the guilt or innocence of the accused violates his due process rights under the Fourteenth Amendment).

¹⁸ Most law enforcement agencies consider face recognition searches to produce “investigative leads” only, not probable cause to make an arrest. But in practice, face recognition matches are often not independently corroborated through additional investigative steps before an arrest is made. See *sup.* note 14.

¹⁹ This represents the general trend currently; some states introduced bills earlier. See, e.g., MD H.B. 1148 (2017).

PROPOSED AND ENACTED LEGISLATION¹

Generally, there have been three legislative approaches to regulating face recognition in the United States: complete bans, moratoria, and regulatory bills. Moratoria can be further broken down into two types: *time-bound moratoria*, which “pause” face recognition use for a set amount of time; and *directive moratoria*, which “pause” face recognition use and require legislative action—such as a task force or express statutory authorization—to supersede the moratoria. Most of these bills have covered all government use of face recognition, with particular attention given to limits placed on police use. This section focuses on police use as well.

Type of legislation	What it does	Examples
Ban	Complete shutdown of all face recognition use	Enacted: San Francisco, CA; ²⁰ Cambridge, MA ²¹ Proposed: Nebraska ²²
Moratorium: time-bound	Face recognition use paused for a set amount of time	Enacted: Springfield, MA ²³ Proposed: Maryland ²⁴
Moratorium: directive	Face recognition use paused, requires legislative action to supersede	Proposed: Massachusetts ²⁵
Regulatory bill	Regulates specific elements of face recognition, along a spectrum from narrowly focused to broader	Enacted: <i>California:</i> prohibited in conjunction with police body-worn cameras ²⁶ (narrower) <i>Washington:</i> regulates numerous elements ²⁷ (broader)

20 See Kate Conger, Richard Fausset, and Serge F. Kovalski, “San Francisco Bans Facial Recognition Technology,” *New York Times*, May 14, 2019, <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>.

21 See Jackson Cote, “Cambridge Bans Facial Recognition Technology, Becoming Fourth Community in Massachusetts to Do So,” *MassLive*, February 27, 2020, <https://www.masslive.com/news/2020/01/cambridge-bans-facial-recognition-technology-becoming-fourth-community-in-massachusetts-to-do-so.html>.

22 See LB1091, “Adopt the Face Surveillance Privacy Act,” Nebraska Unicameral Legislature, available at https://www.nebraskalegislature.gov/bills/view_bill.php?DocumentID=41387.

23 See Jackson Cote, “Springfield City Council Passes Facial Recognition Moratorium,” *MassLive*, February 25, 2020, <https://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html>.

24 MD S.B. 857 (2020), available at <http://mgaleg.maryland.gov/2020RS/bills/sb/sb0857F.pdf>.

25 MA S.B. 1385 (2019), available at <https://malegislature.gov/Bills/191/S1385>.

26 CA A.B. 1215 (2019) (prohibited only until Jan. 1, 2023), available at https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

27 WA Engrossed. Subst. S.B. 6280 (2020), available at <http://lawfilesexst.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf>.

A. Bans¹

The strongest legislative response is to ban the use and acquisition of the technology completely.² Bans can focus on state use of face recognition, commercial or private sector use, or both. To date, only local municipal governments have implemented bans, concentrated in towns and cities in California and Massachusetts. As of July 2020, the following municipalities had banned face recognition: Alameda, California; Berkeley, California; Boston, Massachusetts; Brookline, Massachusetts; Cambridge, Massachusetts; Easthampton, Massachusetts; Northampton, Massachusetts; Oakland, California; San Francisco, California; and Somerville, Massachusetts.²⁸ A number of states proposed bans on face recognition during the 2019–2020 legislative session: Nebraska, New Hampshire, New York, and Vermont.²⁹

City governments have passed bans following robust public dialogue about the risks and benefits of face recognition technology. They represent what is possible with a transparent, democratic process, and the power of proactive localities. In the words of the San Francisco city supervisor who sponsored the ban: “We have an outside responsibility to regulate the excesses of technology precisely because they are headquartered here.”³⁰ It is unclear at this point, however, whether face recognition bans will take hold at the local, state, or federal level. Some jurisdictions may also find the bans to be unintentionally overbroad, restricting uses of the technology deemed to be necessary or uncontroversial.³¹

B. Moratoria⁴

Another strong measure that a legislature can take is to place a moratorium on the technology,³² which has two forms: *time-bound* and *directive*.

-
- 28 See Peter Hegarty, “East Bay City Becomes Latest to Ban Use of Facial Recognition Technology,” *East Bay Times*, December 18, 2019, <https://www.eastbaytimes.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology/>; see Tom McKay, “Berkeley Becomes Fourth U.S. City to Ban Face Recognition in Unanimous Vote,” *Gizmodo*, October 16, 2019, <https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recognition-1839087651>; see Nik DeCosta-Klipa, “Boston City Council Unanimously Passes Ban on Facial Recognition Technology,” *Boston.com*, June 24, 2020, <https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban/>; see ACLU of Massachusetts, “Brookline Bans Municipal Use of Face Surveillance,” December 11, 2019, <https://www.aclum.org/en/news/brookline-bans-municipal-use-face-surveillance>; see sup. note 20; see Michael Connors, “Easthampton Bans Facial Recognition Technology,” *Daily Hampshire Gazette*, July 3, 2020, <https://www.gazettenet.com/Easthampton-City-Council-passes-ordinance-banning-facial-recognition-surveillance-technology-35048140>; see Jackson Cote, “Northampton Bans Facial Recognition Technology, Becoming Third Community in Massachusetts to Do So,” *MassLive*, February 27, 2020, <https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusetts-to-do-so.html>; see CBS SF, “Oakland Officials Take Steps Towards Banning City Use of Facial Recognition Tech,” July 16, 2019, <https://sanfrancisco.cbslocal.com/2019/07/16/oakland-officials-take-step-towards-banning-city-use-of-facial-recognition-tech/>; see sup. note 20; see Alex Newman, “Somerville Bans Facial Recognition Technology,” *Patch*, June 28, 2019, <https://patch.com/massachusetts/somerville/somerville-bans-facial-recognition-technology>.
- 29 NE L.B. 1091 (2020), available at <https://www.nebraskalegislature.gov/FloorDocs/106/PDF/Intro/LB1091.pdf>; NH H.B. 1642 (2020), available at http://gencourt.state.nh.us/bill_status/billText.aspx?sy=2020&id=1202&txtFormat=pdf&v=current; NY S.B. 7572 (2020), available at <https://legislation.nysenate.gov/pdf/bills/2019/S7572>; VT H. 929 (2020), available at <https://legislature.vermont.gov/Documents/2020/Docs/BILLS/H-0929/H-0929%20As%20Introduced.pdf>.
- 30 See sup. note 20.
- 31 See Tim Cushing, “San Francisco Amends Facial Recognition Ban after Realizing City Employees Could No Longer Use Smartphones,” *Techdirt*, December 20, 2019, <https://www.techdirt.com/articles/20191219/18253743605/san-francisco-amends-facial-recognition-ban-after-realizing-city-employees-could-no-longer-use-smartphones.shtml>. The article describes amendments to San Francisco’s ban to permit employees to use the biometric lock feature on city-issued cell phones.
- 32 Moratoria have been used in surveillance policymaking in the past. For example, in 2013, Virginia placed a two-year moratorium on government use of drones. The purpose was to give lawmakers time “to work with law enforcement and other stakeholders to adopt reasonable regulations limiting the use of drones and assuring public participation in the oversight of their use.” See ACLU, “Virginia House of Delegates and Senate Approve Two Year Moratorium on Drones,” February 6, 2013, <https://www.aclu.org/press-releases/virginia-house-delegates-and-senate-approve-two-year-moratorium-drones>.

1. Time-bound moratoria ¹

Time-bound moratoria stop virtually all use of face recognition for a predetermined amount of time.³³ The purpose of this pause is to give elected officials and the public time to learn about face recognition, reconvening later once the moratorium expires. At this point, legislators can decide if, and how, to regulate face recognition. ²

At the municipal level, in early 2020, Springfield, Massachusetts, placed a moratorium on face recognition until 2025.³⁴ At the state level, a 2020 bill introduced in the Maryland legislature would prohibit all public and private use of face recognition for one year.³⁵ The bill does not include any other provisions or directions, but rather states the moratorium “shall remain effective for a period of one year from the date it is enacted and, at the end of the one-year period, this Act, with no further action required by the General Assembly, shall be abrogated and of no further force and effect.”³⁶ ³

Time-bound moratoria raise the possibility for public engagement and the future implementation of either a permanent ban or strong regulation. These bills prompt discussion within legislative committees—the members of which are often unfamiliar with face recognition—about the technology, including its potential harms. There is a risk, however, that if the legislature fails to act once the moratorium period is over, use of face recognition will recommence with no safeguards in place. ⁴

2. Directive moratoria ⁵

Directive moratoria temporarily stop face recognition use while explicitly instructing the legislature or other government officials to take additional steps. Often this entails the creation of a task force, working group, or commission organized by either the legislature or attorney general to study face recognition and recommend policy responses.³⁷ ⁶

A bill introduced in Washington state in 2019 proposed a moratorium on government use of face recognition technology while setting up a task force to study the technology. The task force would be composed of members of historically oversurveilled communities, and would deliver a report to the legislature about potential effects. The bill would also require the attorney general to provide a report certifying the tools in use did not contain accuracy or bias issues, as tested by an independent third party.³⁸ ⁷

33 Time-bound moratoria often have carve-out provisions for face recognition use during emergencies or exigent circumstances and in the case of missing children. Some also have carveouts for use in fraud detection by state driver's licensing departments.

34 Sup. note 23.

35 MA S.B. 0857 (2020), available at <http://mgaleg.maryland.gov/mgaweb/Legislation/Details/sb0857>. Note: the original bill would prohibit government and private use of face recognition for one year. An amendment, discussed at a hearing for the bill, would eliminate the moratorium on private use.

36 Ibid.

37 Provisions creating working groups are often part of non-moratorium regulatory bills, which allow continued use of face recognition until the working group makes further recommendations.

38 WA S.B. 5528 (2019-2020), available at <https://app.leg.wa.gov/bills/summary?BillNumber=5528&Initiative=false&Year=2019>. (Note that this bill is no longer under consideration.)

Directive moratoria can also pause face recognition use *until* the legislature passes certain laws.¹ In contrast to the above example, in which decisions about future policy are left to the working group, this kind of moratorium sets minimum thresholds that future legislation must achieve.

For example, a bill introduced in Massachusetts in 2019 would place a moratorium on government use of biometric surveillance, including face recognition, “[a]bsent express statutory authorization.” That authorization must provide guidance on who is able to use biometric surveillance systems, their purposes, and prohibited uses; standards for data use and management; auditing requirements; and rigorous protections for civil rights and liberties, including compliance mechanisms.³⁹

At the federal level, the *Facial Recognition and Biometric Technology Moratorium Act of 2020* prohibits federal use of certain biometric technologies such as face recognition until Congress explicitly allows their use, with certain limitations. It also conditions federal grant funding to state and local agencies on their adoption of moratoria similar to that proposed in the federal bill.⁴⁰

These bills encourage jurisdictions to research the full implications of face recognition use and engage with members of the public before enacting a more permanent law. Moratoria also limit the risk of reverting to status quo use once the time period is over. However, there is a risk that a task force or commission may not be representative of affected communities; may lack authority; or may be inadequately funded, restricting its effectiveness.⁴¹

C. Regulatory Bills⁵

Regulatory bills seek to place restrictions on face recognition’s use, rather than stop it altogether.⁶ Regulatory bills range along a spectrum from more narrowly focused (regulating only specific uses or other elements of face recognition) to broader (regulating more of these elements).

1. Common elements of regulatory bills⁷

Face recognition bills propose a wide range of measures, including:⁸

- **Task force or working group:** groups must study face recognition and make policy recommendations.
- **Requirements on companies:** face recognition vendors must open up their software to accuracy and bias testing; commercial users must get consent or provide notice of use, as well as allow data access, correction, and removal.

³⁹ MA S.B. 1385 (2019), available at <https://malegislature.gov/Bills/191/S1385>.

⁴⁰ See Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology (June 25, 2020), available at <https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology>.

⁴¹ See, e.g., Governor Jay Inslee, *Letter To the Honorable President and Members, The Senate of the State of Washington* (Mar. 31, 2020), available at <https://crmpublicwebserveice.des.wa.gov/bats/attachment/vetomessage/559a6f89-9b73-ea11-8168-005056ba278b> (vetoing a section of WA S.B. 620 (regulatory bill) that established a face recognition task force on the grounds that it was not funded in the budget).

- **Accountability and transparency reports:** implementing agencies must provide details on the face recognition tools they use, including how and how often, to elected officials. Some require reports before implementation, and many require ongoing reports.⁴² 1
- **Implementing officer process regulations:** officers must receive periodic trainings, conduct meaningful reviews of face recognition search results, and disclose to criminal defendants that face recognition was used in identifying them. 2
- **Explicit civil rights and liberties protections:** such as prohibiting the use of face recognition to surveil people based on characteristics including but not limited to race, immigration status, sexual orientation, religion, or political affiliation. 3
- **Data and access restrictions:** such as prohibiting the sharing of face recognition data with immigration enforcement authorities, limiting federal access to face recognition systems, and prohibiting use on state driver's license databases. 4
- **Targeted bans:** prohibiting specific uses, such as live facial recognition, or in conjunction with body-worn cameras or drones. Face recognition use can also be limited by type of crime—for example, only to investigate violent felonies. 5
- **Court order requirements:** law enforcement must obtain a court order backed by probable cause (or, in some instances, only reasonable suspicion⁴³) to run face recognition searches. Some bills more narrowly apply this requirement to ongoing surveillance or real-time tracking only.⁴⁴ This can also apply narrowly to law enforcement seeking face recognition data from private entities that have collected it, rather than law enforcement searches themselves. 6

2. Examples of regulatory bills 7

A narrower bill proposed in Indiana calls for a “surveillance technology impact and use policy,” but includes no other restrictions.⁴⁵ In New Jersey, a proposed bill requires the attorney general to arrange for third-party accuracy and bias testing.⁴⁶ In 2019, the California legislature passed a law prohibiting “a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera.”⁴⁷ 8

At the other end of the spectrum, broader regulatory bills address multiple elements of face recognition development and use. Though they address a wider range of concerns, this does not mean they necessarily address *all* legitimate areas of concern related to face recognition, or that the proposed rules are substantive or enforceable. 9

42 Some of these provisions are modeled on the federal Wiretap Act. See 18 U.S.C. § 2519, reports concerning intercepted wire, oral, or electronic communications, <https://www.law.cornell.edu/uscode/text/18/2519>.

43 ID H.B. 492 (2020), available at <https://legislature.idaho.gov/sessioninfo/2020/legislation/H0492/>.

44 See, e.g., sup. note 22.

45 IN H.B. 1238 (2020), available at <http://iga.in.gov/legislative/2020/bills/house/1238>.

46 NJ A.B. 989 (2020), available at https://www.njleg.state.nj.us/2020/Bills/A1000/989_11.PDF.

47 CA A.B. 1215 (2019), available at https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215.

For example, in March 2020, Washington state passed a law that regulates numerous elements of face recognition.⁴⁸ The bill includes provisions like these: a pre-implementation accountability report documenting use practices and data management policies for any new face recognition systems; “meaningful human review” when face recognition is used in legal decisions; testing in operational conditions; face recognition service APIs made available for independent accuracy and bias testing; periodic training for officers; mandatory disclosure to criminal defendants; warrants for ongoing, “real-time” or “near-real-time” use; civil rights and liberties protections; and prohibitions against image tampering in face recognition searches.⁴⁹

Regulatory bills seek to strike a balance between the benefits and harms of face recognition use. For example, while a separate privacy bill introduced in Washington in 2019 garnered industry support for its light-touch approach to regulating face recognition, it elicited criticism from privacy advocates for containing loopholes and providing inadequate enforcement mechanisms.⁵⁰ Narrowly targeted bills have a greater likelihood of passing through support from well-resourced law enforcement and company stakeholders, yet often fail to meaningfully protect against the true scope of possible harms.⁵¹ Some advocates are also critical of regulatory bills, particularly more limited ones, for using up available political capital and possibly eliminating the chance of stronger regulation in the future.

CONCLUSION³

In the past year, the United States has turned a significant corner in its approach to face recognition. There is now widespread agreement that regulation is necessary, even as lawmakers, advocates, law enforcement, and other stakeholders may disagree on exactly what that looks like.⁵² The status quo—expansive, unregulated, secret face recognition use—is no longer acceptable.

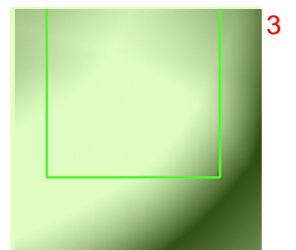
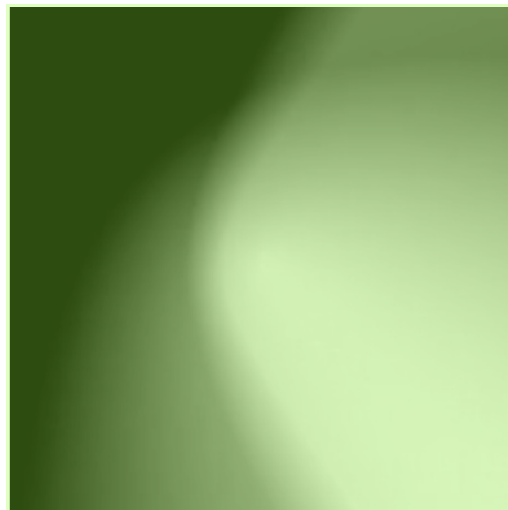
48 See Mariella Moon, “Washington State Approves Stronger Facial Recognition Regulations,” *Engadget*, March 13, 2020, <https://www.engadget.com/2020-03-13-washington-facial-recognition-regulations.html>.

49 Sup. note 27.

50 See Lucas Ropek, “Why Did Washington State’s Privacy Legislation Collapse?,” *Govtech.com*, April 19, 2019, <https://www.govtech.com/policy/Why-Did-Washington-States-Privacy-Legislation-Collapse.html>.

51 See, e.g., Ban Facial Recognition (<https://www.banfacialrecognition.com>), a widely supported petition site calling for a complete ban on police face recognition use.

52 This includes both Republican and Democratic lawmakers, as well as face recognition vendors and law enforcement officials. See, e.g., Shirin Ghaffary, “How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement,” *Vox*, December 10, 2019, <https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation>; see, e.g., Brad Smith, “Facial Recognition: It’s Time for Action,” *Microsoft on the Issues*, December 6, 2018, <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/>; see, e.g., Pat Garrett, “Facial Recognition Technology,” *Washington County Sheriff, Oregon*, June 10, 2020, <https://www.co.washington.or.us/sheriff/CrimePrevention/facial-recognition-technology.cfm>.



BIPA: The Most Important Biometric Privacy Law in the US?

Woodrow Hartzog (Northeastern University)

In May 2020, Clearview AI abruptly ended all service contracts with all non-law enforcement entities based in Illinois.¹ The reason? It hoped to avoid an injunction and potentially large damages under one of the most important privacy laws in America: the Illinois Biometric Information Privacy Act (BIPA).²

Enacted in 2008 in the wake of the bankruptcy of a high-profile fingerprint-scan system, lawmakers designed BIPA to provide “safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric data.”³ It was the first state law in the US to specifically regulate biometrics. Remarkably, as the bill was being deliberated by the Illinois legislature, “there were no questions or discussion, and the bill proceeded immediately to a vote and unanimously passed in the House.”⁴

BIPA’s substantive rules follow a traditional approach to data protection. Compared to omnibus and complex data-protection laws like GDPR, BIPA’s rules are simple. Private entities must get

1 Clearview AI scraped billions of images of people without their permission from social media websites to power their facial recognition app. Clearview filed legal documents in Illinois stating that “Clearview is cancelling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency.” See Ryan Mac, Caroline Haskins, and Logan McDonald, “Clearview AI Has Promised to Cancel All Relationships with Private Companies,” *BuzzFeed*, May 7, 2020, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies>.

2 740 Ill. Comp. Stat. Ann. 14/15.

3 Charles N. Insler, How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act, 43 S. Ill. U. L.J. 819, 820 (2019).

4 Anna L. Metzger, The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy, 50 Loy. U. Chi. L.J. 1051, 1063 (2019).

informed consent before collecting or disseminating a person's biometric information.⁵ They are prohibited from selling, leasing, trading, or otherwise profiting from a person's biometric information.⁶ Companies must also follow specific retention and destruction guidelines.⁷ Finally, the statute binds private entities to a standard of care in transmitting, storing, and protecting biometric information that is equal to or more protective than for other confidential and sensitive information.⁸

While other states such as Texas and Washington have passed standalone biometrics laws,⁹ BIPA² is the only biometric privacy law in the United States with a private cause of action. Multiple states require notice and consent before parties can collect biometric identifiers, require reasonable security measures for covered information, restrict the disclosure of biometric identifiers to specific circumstances, and limit companies' retention of biometric identifiers. But only in Illinois can people who have been aggrieved by companies that violated the rules bring their own action against the alleged violation instead of waiting for the government to file a complaint or levy a penalty.

Given the limited scope of biometric laws, BIPA's private cause of action might not seem monumental—yet it is revelatory in how it has distinguished itself from other biometrics laws. For example, Texas and Washington both authorize their state attorneys general to enforce their biometric privacy laws in ways similar to how states enforce their general data-privacy rules.¹⁰ In contrast, BIPA's private cause of action has meaningfully shaped the practices of companies who deploy biometrics. It has also forced judges to resolve longstanding issues of injury and standing for privacy violations, among the most vexing issues for all privacy-related claims by plaintiffs in civil courts.

Plaintiffs alleging privacy-related harms from things like data breaches, abusive surveillance, and unauthorized disclosure have had a notoriously difficult time in court. Some of this is attributable to the general erosion of access to the American court system through tort reform. Plaintiffs struggle to certify classes for mass litigation, and arbitration clauses are embedded in the ubiquitous terms-of-use agreements online. But a huge roadblock for plaintiffs is the slippery nature of privacy harms.¹¹ Courts have long been skeptical of emotional and reputational

5 740 Ill. Comp. Stat. Ann. 14/15 ("§15(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it [informs the subject what is being collected and receives a written release]... §15(c) (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless [the subject of the biometric identifier or biometric information consents or disclosure is required pursuant to a valid warrant or subpoena]."

6 Id. § 15(c).

7 Id. § 15(a). ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.")

8 Id. § 15(e).

9 Tex. Bus. & Com. Code §503.001; Wash. Rev. Code Ann. §19.375.020; California Consumer Privacy Act (CCPA); N.Y. 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act (broadening information covered by data breach response law to include biometric information); N.Y. Lab. Law §201-a (prohibiting fingerprinting as a condition of employment); Arkansas Code §4-110-103(7) (amending data breach response law to include biometric information).

10 For more information on the role of state attorneys general in privacy policymaking, see Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 748 (2016).

11 M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011); Daniel Solove and Danielle Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Texas Law Review 737 (2018); Ryan Calo, *Privacy Harm Exceptionalism*, 12 J. TELECOMM. & HIGH TECH. L. 361, 361, 364 (2014); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1196 (2015).

damages absent a more obvious physical or financial harm.¹² The Federal Trade Commission, the premier privacy regulator in the US, creates waves when it even hints at the idea that something more than physical or financial harm or extreme emotional suffering should be considered in determining whether particular acts are unfair.¹³ This is to say nothing of the high-stakes debate over whether less specific harms such as anxiety and exposure to risk of data abuses, standing alone, can constitute an actionable injury in the context of claims of negligence which led to a data breach.¹⁴

But most discrete and individual privacy encroachments are not catastrophic. The modern privacy predicament is more akin to death by a thousand cuts. Small intrusions and indiscreet disclosures could lead to compromised autonomy, obscurity, and trust in relationships. What's more, it can be difficult to specifically articulate and identify the ways in which data breaches make us more vulnerable. Torts require a clear line of causation from fault to harm. That's usually relatively easy to prove with things like physical injuries from car wrecks, though it is less so with data breaches. Even if it's clear that a malicious actor has gained access to peoples' information, criminals don't always straightforwardly use data obtained from a breach to inflict direct financial or emotional injury upon the data subject. They often aggregate the information in a pool for further exploitation or sit on it for years so as not to arouse suspicion. Often people have no idea who wronged them online. American data-privacy law simply isn't built to respond to this kind of diffuse and incremental harm.¹⁵

BIPA has spurred a key intervention into this morass. Specifically, with BIPA, several judicial opinions have affirmed the argument that regardless of whether wrongful acts with biometric information resulted in chilling effects or financial or emotional injury, the collection and processing of biometric data without notice and consent is alone a cognizable injury because it is an affront to a person's dignity and autonomy. Two cases in particular demonstrate the importance of BIPA.

In *Rosenbach v. Six Flags Entm't Corp.*, a mother brought a claim on behalf of her son against Six Flags amusement park for the company's failure to give notice or obtain consent when collecting the child's fingerprints for their biometric identification system.¹⁶ At issue was whether the plaintiffs alleged sufficient actual or threatened injury to have standing to bring suit. Plaintiffs did not allege financial or extreme emotional harm, but rather a harm resulting solely from the prohibited collection and processing of personal biometric data without making the required

¹² Id.

¹³ See *F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 623 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) ("The parties contest whether non-monetary injuries are cognizable under Section 5 of the FTC Act....Although the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue....").

¹⁴ Daniel Solove and Danielle Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Texas Law Review 737 (2018).

¹⁵ Daniel J. Solove and Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737, 762 (2018) ("Hackers may not use the personal data in the near term to steal bank accounts and take out loans. Instead, they may wait until an illness befalls a family member and then use personal data to generate medical bills in a victim's name. They may use the personal data a year later but only use some individuals' personal information for fraud.").

¹⁶ *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 8, 129 N.E.3d 1197, 1200–01 ("The complaint alleges that this was the first time Rosenbach learned that Alexander's fingerprints were used as part of defendants' season pass system. Neither Alexander, who was a minor, nor Rosenbach, his mother, were informed in writing or in any other way of the specific purpose and length of term for which his fingerprint had been collected. Neither of them signed any written release regarding taking of the fingerprint, and neither of them consented in writing 'to the collection, storage, use sale, lease, dissemination, disclosure, redisclosure, or trade of, or for [defendants] to otherwise profit from, Alexander's thumbprint or associated biometric identifiers or information.'").

disclosures or obtaining written consent. The Appellate Court of Illinois held that “a plaintiff is not ‘aggrieved’ within the meaning of the Act and may not pursue either damages or injunctive relief under the Act based solely on a defendant’s violation of the statute. Additional injury or adverse effect must be alleged.”¹⁷ However, the Supreme Court of Illinois disagreed. 1

Chief Justice Lloyd A. Karmeier, writing the opinion of the court, noted that if the Illinois legislature had wanted to impose an injury requirement beyond disclosure and consent failures, they likely would have done so, as they have in other legislation.¹⁸ Using accepted principles of statutory construction, the court interpreted BIPA’s language that “[a]ny person aggrieved by a violation of this Act shall have a right of action” according to its commonly understood legal meaning. Specifically, they found that “to be aggrieved simply ‘means having a substantial grievance; a denial of some personal or property right.’”¹⁹ Justice Karmeier wrote, “A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as ‘aggrieved.’”²⁰ 2

The court in *Rosenbach* found that Six Flags violated BIPA’s “right to privacy in and control over their biometric identifiers and biometric information.”²¹ BIPA’s disclosure and consent requirements give shape to that right. Thus, if a company violates BIPA, then the data subject is legally “aggrieved” because their right to privacy in and control over their biometric data has been compromised.²² 3

Perhaps the most significant passage in *Rosenbach* concerned the court’s response to the defendant’s argument that its BIPA violations were merely “technical” in nature. The court argued that such a characterization misunderstands not only what the legislature was trying to accomplish but also the unique nature of how biometrics threaten peoples’ privacy and how procedural rules mitigate that threat. “The Act vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent.”²³ Peoples’ unique biometric identifiers, now easily wholesale collected and stored, are not like other kinds of authenticators like passwords and social security numbers because if they are compromised, they cannot be changed. Even beyond identity theft, the court noted that biometrics are particularly concerning because their full risks are not known. The court was direct in its finding: 4

17 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 15, 129 N.E.3d 1197, 1202 (citing *Rosenbach v. Six Flags Entm’t Corp.*, 2017 IL App (2d) 170317, rev’d, 2019 IL 123186, 129 N.E.3d 1197).

18 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 25, 129 N.E.3d 1197, 1204. (“Defendants read the Act as evincing an intention by the legislature to limit a plaintiff’s right to bring a cause of action to circumstances where he or she has sustained some actual damage, beyond violation of the rights conferred by the statute, as the result of the defendant’s conduct. This construction is untenable. When the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear.”).

19 *Id.* (citing *Glos v. People*, 259 Ill. 332, 340, 102 N.E. 763 (1913)).

20 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 30, 129 N.E.3d 1197, 1205 (“Rather, ‘[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment.’”) (citing *Glos v. People*, 259 Ill. 332, 340, 102 N.E. 763 (1913)).

21 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206.

22 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (“No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual’s or customer’s statutory cause of action.”).

23 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 34, 129 N.E.3d 1197, 1206.

When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, “the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.”...This is no mere “technicality.” The injury is real and significant.²⁴

The court also highlighted how integral a private cause of action was in implementing the legislature’s privacy goals for BIPA. When companies face liability for legal violations without burdening plaintiffs to show some additional injury, “those entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone.”²⁵ The court noted that the cost of complying with BIPA is “likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced.”²⁶ According to the court, to force plaintiffs to wait until they could prove some sort of financial or emotional harm would counteract BIPA’s prevention and deterrence goals.

The other case illustrative of BIPA’s potency, *Patel v. Facebook*,²⁷ involves federal standing doctrine as required by Article III of the US Constitution, a concept linked to injury and harm thresholds. Standing doctrine requires that plaintiffs “must have suffered an ‘injury in fact’—an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical.”²⁸ In a landmark 2016 US Supreme Court case, *Spokeo, Inc. v. Robins* affirmed that an injury-in-fact for information-related complaints like those against data brokers for mishandling, inaccuracies, and indiscretion must be “concrete,” though the court was frustratingly vague about what kinds of harms met that threshold.²⁹

Patel v. Facebook involved a complaint that Facebook violated BIPA with its use of facial recognition tools. The Ninth Circuit applied a two-part test to determine “(1) whether the statutory provisions at issue were established to protect [the plaintiff’s] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests.”³⁰ The Ninth Circuit answered yes to both questions.

In determining that BIPA protected a concrete interest rather than a purely procedural protection, the Ninth Circuit noted that privacy rights have long served as the basis for legal action in the common law, constitutional law, and in statutes at both the state and federal level. The court noted the significant vulnerabilities created by facial recognition technology:

24 *Id.*
25 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 37, 129 N.E.3d 1197, 1206.

26 *Id.*

27 *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020).

28 *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992).

29 *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548–49, 194 L. Ed. 2d 635 (2016), as revised (May 24, 2016). (“When we have used the adjective ‘concrete,’ we have meant to convey the usual meaning of the term—‘real,’ and not ‘abstract.’...Concreteness, therefore, is quite different from particularization. ‘Concrete’ is not, however, necessarily synonymous with ‘tangible.’ Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.”) The Court went on to muddy the waters in *Spokeo* even further, writing, “Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, [Plaintiff] could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III...This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness.” *Id.* at 1549.

30 *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1270–71 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (citing *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017) (*Spokeo II*)).

[T]he facial-recognition technology at issue here can obtain information that is “detailed, encyclopedic, and effortlessly compiled,” which would be almost impossible without such technology...Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual’s Facebook friends or acquaintances who are present in the photo...[It] seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual’s cell phone.³¹

The court concluded that “the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual’s private affairs and concrete interests. Similar conduct is actionable at common law.”³² The court cited the language in *Rosenbach* in holding that “the statutory provisions at issue’ in BIPA were established to protect an individual’s ‘concrete interests’ in privacy, not merely procedural rights,” and that by alleging a BIPA violation the “the plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing.”³³

BIPA has a number of virtues. Thanks to BIPA’s private cause of action, it has become the key for holding companies that use biometric systems accountable.³⁴ In the absence of a private cause of action, enforcement of biometrics and consumer protection laws is generally left to state attorneys general (AG). While state AGs are certainly key to privacy policymaking in the US, they have limited resources and a host of issues on their plate.³⁵ Even with unlimited bandwidth, state AGs have limited legal ability and political capital to extract the kind of fines necessary to sufficiently deter companies. The same holds true for the Federal Trade Commission, which is America’s primary privacy regulator.³⁶

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook’s share price actually rose 2 percent after the FTC announced its historic \$5 billion fine for the social media company’s privacy lapses in the Cambridge Analytica debacle.³⁷ Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts.³⁸ On top of that, Clearview AI is being sued by the ACLU for violating

31 *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (citations omitted). BIPA’s focus on face templates as a creation that grants surveillance and other affordances is properly distinguished from a standard photograph, which does not provide the same affordance of serving as a beacon.

32 *Id.*

33 *Id.* at 1274.

34 Over three hundred class action lawsuits have been brought under BIPA as of June 2019. See Seyfarth Shaw, “Biometric Privacy Class Actions by the Numbers: Analyzing Illinois’ Hottest Class Action Trend,” Seyfarth, June 28, 2019, <https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/>.

35 See Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 *Notre Dame L. Rev.* 747 (2016).

36 See Daniel Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 *Columbia Law Review* 583 (2014); Woodrow Hartzog and Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 *George Washington Law Review* 2230 (2015).

37 Charlotte Jee, “Facebook Is Actually Worth More Thanks to News of the FTC’s \$5 Billion Fine,” *MIT Technology Review*, July 15, 2019, <https://www.technologyreview.com/2019/07/15/134196/facebook-is-actually-richer-thanks-to-news-of-the-ftcs-5-billion-fine/>.

38 Nick Statt, “Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies,” *Verge*, May 7, 2020, <https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law>.

BIPA by creating faceprints of people without their consent.³⁹ It is no wonder that the private cause of action is one of two reasons the United States does not have an omnibus federal data privacy law (the other being federal preemption of state privacy frameworks).⁴⁰ In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.⁴¹

Even given BIPA's virtues and remarkable effectiveness, it is probably not the best model for America's biometric privacy identity. A private cause of action is necessary, but not sufficient, to respond to the risk of biometrics. BIPA is rooted in a myopic and atomistic "notice and choice" approach to privacy.

There are two major problems with building a biometric privacy framework almost exclusively around concepts of transparency and informational self-determination. First, by focusing on giving people control over their data and mandating procedural disclosure obligations, these frameworks fail to impose substantive limits on how far companies can encroach into our lives and how deeply these systems can be entrenched. Procedural transparency and consent regimes end up serving as a justification mechanism for all kinds of encroachments without any clear backstop to how vulnerable we can be made to these systems, so long as we consent. Furthermore, BIPA fails to address the issues around privacy in public spaces or in data that already has been exposed to the public. For example, judges considering privacy claims have said repeatedly that "there can be no privacy in that which is already public."⁴²

Privacy is about more than just informational self-determination. It is about trust, dignity, freedom from oppression, and laying the preconditions for human flourishing. But those values are not necessarily reflected in the net outcome of billions of individual decisions. Moreover, companies create structured environments that can heavily influence these discrete choices, with powerful incentives to get us to say "yes" any way they can.⁴³

39 ACLU, American Civil Liberties Union, American Civil Liberties Union of Illinois, Chicago Alliance Against Sexual Exploitation, Sex Workers Outreach Project Chicago, Illinois State Public Interest Research Group, Inc., and Mujeres Latinas en Acción v. Clearview AI, Inc., https://www.aclu.org/sites/default/files/field_document/aclu_v_clearview_complaint_final.pdf.

40 See Makena Kelly, "Congress Is Split over Your Right to Sue Facebook," *Verge*, December 3, 2019, <https://www.theverge.com/2019/12/3/20993680/facebook-google-private-right-of-action-sue-data-malpractice-wicker-cantwell>; and Emily Birnbaum, "Lawmakers Jump-Start Talks on Privacy Bill," *The Hill*, August 7, 2019, <https://thehill.com/policy/technology/456459-lawmakers-jump-start-talks-on-privacy-bill>; and Ben Kochman, "Senate Privacy Hearing Zeroes in on Right to Sue, Preemption," *Law360*, December 4, 2019 (paywall), <https://www.law360.com/articles/1224809/senate-privacy-hearing-zeroes-in-on-right-to-sue-preemption>; and Cameron F. Kerry, John B. Morris, Caitlin Chin, and Nicol Turner Lee, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," *Brookings*, June 3, 2020, <https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/>.

41 See Issie Lapowsky, "New York's Privacy Bill Is Even Bolder than California's," *Wired*, June 4, 2019, <https://www.wired.com/story/new-york-privacy-act-bolder/>; DJ Pangburn, "How Big Tech Is Trying to Shape California's Landmark Privacy Law," *Fast Company*, April 25, 2019, <https://www.fastcompany.com/90338036/how-big-tech-is-trying-to-shape-californias-landmark-privacy-law>; John Hendel and Cristiano Lima, "Lawmakers Wrangle over Consumer Lawsuits as Privacy Talks Drag," *Politico*, June 5, 2019, <https://www.politico.com/story/2019/06/05/privacy-advocates-consumer-lawsuits-1478824>; and "Potentially Expanded Private Right of Action Increases Risk of Class Action Exposure under the California Consumer Privacy Act," *Dorsey*, May 1, 2019, <https://www.dorsey.com/newsresources/publications/client-alerts/2019/04/private-right-of-action-increases-risk>.

42 Woodrow Hartzog, *The Public Information Fallacy*, 98 *Boston University Law Review* 459 (2019). The FBI alleges it does not need permission to conduct surveillance using powerful technologies like cell-site simulators (often called "Stingrays"), so long as they are doing so in public places. Judges have refused to punish people for taking "upskirt" photos because the women photographed have no reasonable expectation of privacy "in public," no matter how fleeting their exposure. *Id.*

43 Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, MA: Harvard University Press, 2018).

BIPA is simply not capable of providing individuals with meaningful agency over modern data practices.⁴⁴ “Informed consent” is a broken privacy regulatory mechanism.⁴⁵ It doesn’t scale, it offloads risk onto the person giving the consent, and it is easily manufactured by companies who control what we see and what we can click. Companies deploy malicious user interfaces and a blizzard of dense fine print to overwhelm our decision-making process. Consent regimes give the illusion of control while justifying dubious practices that people don’t have enough time or cognitive resources to understand. Even if people were able to adequately gauge the risks and benefits of consenting to biometric practices, they often don’t have a meaningful choice in front of them since they cannot afford to say no and decline a transaction or relationship. While people should be protected regardless of what they consent to, BIPA is largely agnostic to the post-permission risks of biometric technologies.

1

BIPA is far more effective than any other law on the books in protecting our biometric privacy with respect to private companies. However, it does not confront the structural change and substantive limits necessary for a sustainable future with biometric technologies. BIPA allows companies to exploit people as their consent is harvested through systems designed to have them hurriedly click “I Agree” and get on with their busy lives. BIPA’s success entrenches an overly individualistic and procedural approach to privacy, but has shown lawmakers what is indispensable in a biometric privacy framework. It is a guide not just because of what it provides but also because of what it lacks.

2

44 Woodrow Hartzog, The Case Against Idealising Control, 4 European Data Protection Law Review 423 (2018).

45 Neil Richards and Woodrow Hartzog, The Pathologies of Digital Consent, 96 Washington University Law Review 1461 (2019); Evan Selinger and Woodrow Hartzog, The Inconsentability of Facial Surveillance, 66 Loyola Law Review 101 (2019).

Bottom-Up Biometric Regulation: A Community's Response to Using Face Surveillance in Schools¹

Stefanie Coyle (NYCLU)

Rashida Richardson (Rutgers University, AI Now Institute, NYU)²

Public schools are increasingly turning to invasive technological solutions to address a wide range of school safety issues. Because events like school shootings are both nuanced and politically or socially charged, school administrators often rush to embrace technological tools without proper consideration or community consultation. The risks, concerns, and bureaucratic pitfalls of this approach are most salient in the context of biometric technologies used in schools. This case study examines the controversial move by a school district in Lockport, New York, to implement a facial and object-recognition system, and the community-driven response that sparked a national debate and led to state-wide legislation regulating the use of biometric technologies in schools.³

FACIAL RECOGNITION SURVEILLANCE IN SCHOOLS⁴

Surveillance technologies are becoming a norm in many public schools.¹ School administrators are turning to a rapidly growing market of “free”² or subsidized tools that monitor student emails for concerning phrases, measure student bathroom breaks, proctor exams, or provide real-time⁵

¹ Circumstances leading to increased adoption of surveillance technologies in schools may vary by country. This chapter focuses on the United States.

² RealNetworks, Inc., “RealNetworks Provides SAFR Facial Recognition Solution for Free to Every K–12 School In the United States and Canada,” July 18, 2018, <https://www.prnewswire.com/news-releases/realnetworks-provides-safr-facial-recognition-solution-for-free-to-every-k-12-school-in-the-us-and-canada-300681977.html>.

alerts of potential crises,³ often without proper consideration or community consultation. School administrators have shown significant interest in biometric and other access-control technologies for targeting nuanced school safety issues, with few existing regulations to hold them back.⁴ In 2019, *Wired* “identified eight public school systems, from rural areas to giant urban districts, that have moved to install facial recognition systems,” though national use statistics remain unknown.⁵

Because these technologies can be enabled as “add-on” features or easily integrated with existing systems used by a school or school district (e.g., closed-circuit television), administrators often adopt or test them without fully considering the risks they entail.⁶ For example, school administrators may face legal obligations regarding the storage and use of biometric data, and may not have policies in place to deal with a data breach or sufficient funding available for maintenance of these systems.

Biometric technologies present a veneer of social control or risk mitigation,⁷ but in reality they pose unique social and legal concerns for students, particularly in the K–12 setting. Though students have some enhanced data-privacy protections and greater expectations regarding government oversight and enforcement,⁸ they are particularly vulnerable because the consequences of privacy and other legal violations may not be immediately felt or obvious. Moreover, for decades, critical scholars and educators have criticized these types of reactionary educational policies and practices because they are not long-term solutions. Indeed, they tend to reproduce, maintain, and naturalize structural inequities that pervade the American education system and allow policymakers to avoid necessary structural reforms.⁹

Internationally, some national authorities have opposed facial recognition and other biometric technologies in schools, finding some uses in schools to be unlawful although not banning the

3 Meghna Chakrabarti and Hilary McQuilkin, “When Schools Use Tech to Monitor Students Online, Class Is Always in Session,” *WBUR*, October 31, 2019, <https://www.wbur.org/onpoint/2019/10/31/school-surveillance-students-online-privacy-safety>.

4 The last substantive guidance on the Family Educational Rights and Privacy Act (FERPA) from the United States Department of Education was issued in 2007; it described the application of FERPA to the use of security videos and the transfer of educational records. US Department of Education, “Balancing Student Privacy and School Safety: A Guide to the Family Educational Rights and Privacy Act for Elementary and Secondary Schools,” October 2007, <https://www2.ed.gov/policy/gen/guid/fpco/brochures/elsec.html>.

5 Tom Simonite and Gregory Barber, “The Delicate Ethics of Using Facial Recognition in Schools,” *Wired*, October 17, 2019, <https://www.wired.com/story/delicate-ethics-facial-recognition-schools/>.

6 Bart Simon, “The Return of Panopticism: Supervision, Subjection and the New Surveillance,” *Surveillance & Society* 3, no. 1 (September 1, 2002): 1–20, <https://doi.org/10.24908/ss.v3i1.3317>. Simon notes that individuals perform compliance around surveillance technologies, which makes assessing broader, long-term efficacy or value difficult. See also Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* (Oxford: Berg, 1999). The authors discuss how public surveillance systems have inherent blind spots that diminish effectiveness or intended goals.

7 Andrew Hope, “Seductions of Risk, Social Control, and Resistance to School Surveillance,” in *Schools Under Surveillance: Cultures of Control in Public Education*, eds. Torin Monahan, R. Torres, and Aaron Kupchik (New Brunswick: Rutgers University Press, 2009), 230–235.

8 See, e.g., Family Educational Rights Privacy Act (FERPA), 20 U.S.C. § 1232g; Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h; Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506; Individuals with Disabilities Education Act (IDEA), 20 U.S.C. § 1400 et seq; Children’s Internet Protection Act (CIPA), 47 CFR § 54.520; National School Lunch Act, 42 U.S.C. § 1751 (2008). Several states have additional student privacy laws. FERPA/SHERPA, State Student Privacy Laws (2019), <https://ferpasherpa.org/state-laws/> (updated Aug. 6, 2019).

9 See, e.g., Daniel Kiel, “No Caste Here? Toward a Structural Critique of American Education,” *Penn State Law Review* 119, no. 3 (2015): 611–644, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2738704. Kiel argues that colorblind classification methods in education policy help maintain racial hierarchies in society and insulate educational institutions from legal, political, and practical interventions. See also Jason P. Nance, “Student Surveillance, Racial Inequalities, and Implicit Racial Bias,” *Emory Law Journal* 66, no. 4 (2017): 765–837. Nance documents the ways in which intensified school surveillance practices and policies disproportionately and negatively affect students of color. See also David Gillborn, “Education Policy as an Act of White Supremacy: Whiteness, Critical Race Theory and Education Reform,” *Journal of Education Policy* 20, no. 4 (2005): 485–505, <https://doi.org/10.1080/02680930500132346>. Gillborn argues that educational policy in the United Kingdom reinforces and facilitates racial inequities.

use of the technology in other settings.¹⁰ At the same time, several states and localities have passed or are considering laws that will ban government use of facial recognition technologies, which applies to public schools.¹¹ US civil society organizations Fight for the Future and Students for Sensible Drug Policy created a campaign to ban use of facial recognition technology on college campuses.¹² This campaign successfully forced the University of California Los Angeles (UCLA) to reverse its plans to implement facial recognition for campus security,¹³ and has garnered support from teachers' unions that are expanding the campaign's call to extend to K–12 schools.¹⁴

In 2019, New York became the first state to introduce legislation that explicitly sought to bar school districts from purchasing biometric surveillance technologies, and directed the State Education Commissioner to conduct a study on the use of such technologies in schools and issue statewide recommendations.¹⁵ This legislation was in response to and in collaboration with a community-led advocacy effort in Lockport, New York.

LOCKPORT, NEW YORK: A CASE STUDY IN COMMUNITY-DRIVEN PUSHBACK TO FACIAL RECOGNITION IN SCHOOLS

In 2014, New York voters approved the Smart Schools Bond Act (SSBA), which set aside \$2 billion for school districts to “improve learning and opportunity for students throughout” New York State.¹⁶ An inconspicuous provision within the SSBA allowed school districts to utilize the

- 10 The Administrative Court of Marseille (https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf) found that the use of facial recognition gates in two French high schools without student consent violated GDPR, despite national government interest in establishing a legal framework for public biometric video surveillance. See also European Data Protection Board, “Facial Recognition in Schools Renders Sweden’s First GDPR Fine,” August 22, 2019, https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en. The article discusses the issuing of Sweden’s first GDPR fine for failure to perform an adequate impact assessment and unlawful processing of sensitive biometric data to a municipality that used facial recognition technology to monitor student attendance. And see Scottish Government, “Biometric Technologies in Schools: Draft Guidance for Education Authorities, September 9, 2008, <http://www.scotland.gov.uk/Publications/2008/09/08135019/0>. The document discourages educational authorities from adopting biometric technologies but does not rescind preexisting findings that biometric technologies in schools are not illegal, even when introduced without parental consultation.
- 11 See Kristin Lam, “Portland, the Largest City in Oregon, Plans to Propose First Facial Recognition Ban Affecting Private Companies,” *USA Today*, December 3, 2019, <https://www.usatoday.com/story/tech/2019/12/03/facial-recognition-portland-oregon-ban/2601966001/>; Tom McKay, “Berkeley Becomes Fourth U.S. City to Ban Face Recognition in Unanimous Vote,” *Gizmodo*, October 16, 2019, <https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651>; City and County of San Francisco Board of Supervisors, File # 190110, May 31, 2019, <https://sfgov.legistar.com/LegislationDetail.aspx?ID=3850006&GUID=12FC5DF6-AAC9-4F4E-8553-8F0CD0EBD3F6>; Christine Fisher, “Oakland Bans City Use of Facial Recognition Software,” *Engadget*, July 17, 2019, <https://www.engadget.com/2019/07/17/oakland-california-facial-recognition-ban/>; ACLU Massachusetts, “Somerville City Council Moves to Ban Government Face Surveillance,” June 24, 2019, <https://www.aclum.org/en/news/somerville-city-council-moves-ban-government-face-surveillance>.
- 12 Stop Facial Recognition on Campus, <https://www.banfacialrecognition.com/campus/>.
- 13 Lilah Burke, “Facial Recognition Surveillance on Campus,” *Inside Higher Ed*, February 21, 2020, <https://www.insidehighered.com/news/2020/02/21/ucla-drops-plan-use-facial-recognition-security-surveillance-other-colleges-may-be>.
- 14 Boston Teachers Union (@BTU66), “The BTU joins with teachers, students, civil rights and immigrant rights groups across the nation today in support of a ban on dangerous and inaccurate facial recognition technology in schools and universities,” Twitter, March 2, 2020, 4:37 p.m., <https://twitter.com/BTU66/status/1234593709267865603>.
- 15 Assembly Bill A6787-D (2019–20), <https://www.nysenate.gov/legislation/bills/2019/a6787>.
- 16 Smart Schools Bond Act (2014), http://www.p12.nysed.gov/mgt/serv/smart_schools/home.html.

funds on “high-tech security” projects, with little guidance. The SSBA is a reimbursement scheme that requires school districts to submit proposals and records of community engagement to the Smart Schools Review Board for review and approval.¹⁷

Since 2014, many school districts have applied for and obtained reimbursement for funding to acquire student instructional technology, such as laptops, smart boards, and 3D printers, and to upgrade aging internet and Wi-Fi systems.¹⁸ As part of the application process, districts must certify that they have engaged stakeholders on the projects—specifically requiring that parents, students, teachers, and the community be notified of the project. Districts are also required to hold a public hearing about the proposals and post the proposal documentation on the district's website for at least thirty days.¹⁹ Ostensibly, these requirements are designed to ensure that school community members are able to give input about the wisdom of the district's proposed use of state funding.

In 2016, the Lockport City School District proposed the use of \$3,810,833 in SSBA funds for “new cameras and wiring...to provide viewing and automated facial and object recognition of live and recorded surveillance video,” as well as “additional surveillance servers...to provide enhanced storage of recorded video and processing.”²⁰ Lockport allegedly purchased the system to prevent school shootings.²¹ It held its required public hearing on the proposal in the middle of summer break; unsurprisingly, it did not receive any comments or questions from the community about the purchase.²² Lockport certified that it had engaged with all required stakeholders and its proposal was approved by the Smart Schools Review Board in November 2017.²³

The first public criticism of the project started in February 2018 when the local newspaper, the *Lockport Union-Sun & Journal*, published a piece on one of two resolutions approved at the February 2018 Lockport school board meeting.²⁴ The resolution was to allow the use of “a new facial and shape recognition software” in the school system.²⁵ Lockport resident and parent Jim Shultz was alarmed by the revelation and wrote an article in his opinion column for the newspaper questioning the need for such a system, underscoring other, better uses for the funds, and

17 The makeup of the Smart Schools Review Board is governed by statute and is comprised of the Commissioner of the New York State Education Department, the Director of the Office of the Budget, and the Chancellor of the State University of New York system, or their designees. N.Y. Educ. Law § 3641(16)(a)(2).

18 Approved Smart Schools Investment Plans, http://p1232.nysed.gov/mgtserv/smart_schools/ApprovedSSIPs.htm. See, e.g., Adirondack Central School District's request for upgrades to wireless connectivity and Chromebooks for students (http://p1232.nysed.gov/mgtserv/documents/ADIRONDACKCSD_ADKInvestmentPlan11.16.pdf).

19 Smart Schools Bond Act Implementation Guidance, p. 19, http://www.p12.nysed.gov/mgtserv/documents/SSBAGuidancerev_6_1_18_Final.pdf.

20 Lockport City School District, Smart Schools Investment Plan (2016–17), <http://p1232.nysed.gov/mgtserv/documents/LOCKPORTCITYSD.pdf> (last modified October 23, 2017).

21 Lockport City School District, Aegis Security System, May 2019, <https://www.smores.com/q13ms>.

22 Lockport City School District, August 2016 Regular Board Meeting Minutes, August 17, 2016, <https://www.lockportschools.org/site/default.aspx?PageType=14&DomainID=1298&PageID=9632&ModuleInstanceID=11244&ViewID=1e008a8a-8e8a-4ca0-9472-a8f4a723a4a7&IsMoreExpandedView=True>.

23 Governor Andrew M. Cuomo, “Governor Cuomo Announces Approval of 88 Smart Schools Investment Plans Totaling \$75.6 Million,” November 27, 2017, <https://www.governor.ny.gov/news/governor-cuomo-announces-approval-88-smart-schools-investment-plans-totaling-756-million>. Despite the district's certification, David Lowry, the president of the Lockport Education Association, stated that teachers were not consulted in a discussion of how to use the funding, as was required. See Tim Fenster, “Trying for More Secure Schools: Lockport District Turning to Facial Recognition Software,” *Lockport Union-Sun & Journal*, March 4, 2018, http://www.lockportjournal.com/news/local_news/trying-for-more-secure-schools-lockport-district-turning-to-facial/article_f1cc9cfa-0898-5da0-ac5d-d600df21bed7.html.

24 Connor Hoffman, “Lockport Schools Look to Cut Energy Costs,” *Lockport Union-Sun & Journal*, February 8, 2018, https://www.lockportjournal.com/news/local_news/lockport-schools-look-to-cut-energy-costs/article_6374faf0-7c5b-57d9-bc37-a1542df857a5.html.

25 Ibid.

warning of the risks to privacy for students and teachers.²⁶ Shultz created a petition asking the school district to put the project on hold and to schedule a public hearing to receive input from the community.²⁷ The petition, signed by over a hundred Lockport residents, raised additional questions about the district's engagement with stakeholders, potential conflicts of interest between the district and the security consultant that pitched the product, and the effectiveness of the system.²⁸

After the petition was turned in, the *Lockport Journal* editorial board called on the district to postpone its scheduled vote to award an installation contract for the system.²⁹ Despite this call to action, the Lockport school board approved the contract.³⁰ Shultz then called for residents to vote down Lockport's proposed school budget until the district agreed to stop its facial recognition proposal, but was unsuccessful.³¹ The *Lockport Journal*, however, continued to run pieces on the dangers of facial recognition technology, questioning its accuracy and, in particular, discrepancies in the systems' ability to identify people of color.³² Shultz wrote monthly columns about the project, and enlisted local support through Lockport's Facebook group. He also solicited the help of the New York Civil Liberties Union, which targeted the district and the New York State Education Department (NYSED) with letters and requests under New York's freedom of information law.³³

This advocacy garnered the attention of Monica Wallace, Democrat Assembly member representing New York's 143rd Assembly District, which borders Lockport and includes the town of Depew.³⁴ Wallace was aware of the school district's proposal because the superintendent of the Depew Union Free School District had expressed interest in obtaining the same system.³⁵ Wallace reached out to advocates in an effort to understand the concerns. As a lawyer and parent, she understood the tension between safety and privacy, but worried that the system had the potential to do more harm than good.

- 26 Jim Shultz, "Lockport Schools' Security Plan Warrants Scrutiny," *Lockport Union-Sun & Journal*, February 21, 2018, https://www.lockportjournal.com/opinion/lockport-schools-security-plan-warrants-scrutiny/article_34f86bd0-849c-5251-8e73-387b90af357b.html.
- 27 Jim Shultz, "More Questions about School Surveillance Plan," *Lockport Union-Sun & Journal*, March 21, 2018, https://www.lockportjournal.com/opinion/more-questions-about-school-surveillance-plan/article_0c5c6948-cded-5fe2-8d9c-c3e145ae2ed4.html.
- 28 Ibid.
- 29 US&J Editorial Board, "OUR VIEW: Action on School Security Bid Should Be Postponed," *Lockport Union-Sun & Journal*, March 28, 2018, https://www.lockportjournal.com/opinion/our-view-action-on-school-security-bid-should-be-postponed/article_464b8f55-733e-554f-9ddb-c066ab3ce169.html.
- 30 Minutes of the Board of Education of the Lockport City School District, March 28, 2018, <https://www.lockportschools.org/site/default.aspx?PageType=14&DomainID=1298&PageID=9632&ModuleInstanceID=11844&ViewID=1e008a8a-8e8a-4ca0-9472-a8f4a723a4a7&IsMoreExpandedView=True>.
- 31 Jim Shultz, "Vote 'No' on Spy Cameras in Lockport's Schools," *Lockport Union-Sun & Journal*, April 25, 2018, https://www.lockportjournal.com/opinion/vote-no-on-spy-cameras-in-lockports-schools/article_6c8cf70a-9551-5974-b396-67bfb5672789.html; Jim Shultz, "Reject False Security: Vote 'No' on Lockport School Budget," *Lockport Union-Sun & Journal*, May 11, 2018, https://www.lockportjournal.com/opinion/reject-false-security-vote-no-on-lockport-school-budget/article_672a7a72-4908-588e-bccc-0cddaf4683b0.html.
- 32 Tim Fenster, "Questions remain on school district security project," *Lockport Union-Sun & Journal*, May 13, 2018, https://www.lockportjournal.com/news/local_news/questions-remain-on-school-district-security-project/article_97ce6fd3-490e-5837-834b-217b29474ee5.html.
- 33 See Connor Hoffman, "Civil Liberties Union Asks State to Halt Lockport Schools Security Project," *Lockport Union-Sun & Journal*, June 18, 2018, https://www.lockportjournal.com/news/local_news/civil-liberties-union-asks-state-to-halt-lockport-schools-security/article_dbf50305-cd3a-54d9-8757-4c874c02c61b.html; Stefanie D. Coyle and John A. Curr III to Commissioner MaryEllen Elia, June 18, 2018, https://www.nyclu.org/sites/default/files/field_documents/june18_2018_nyclu_letter_re_lockport_city_school_district.pdf.
- 34 Assemblymember Monica P. Wallace, <https://assembly.state.ny.us/mem/Monica-P-Wallace/about/>.
- 35 Thomas J. Prohaska, "Lockport Schools Turn to State-of-the-Art Technology to Beef up Security," *Buffalo News*, May 20, 2018, <https://buffalonews.com/2018/05/20/lockport-schools-turn-to-state-of-the-art-technology-to-beef-up-security/>.

1 In March 2019, Wallace introduced a bill (A6787) in the New York State Assembly that would place a moratorium on the use or purchase of any “biometric identifying technology” in a school system.³⁶ This broad definition covers not only facial recognition technology, but any technology that uses a fingerprint, handprint, iris, retina, DNA sequence, voice, gait, or facial geometry to identify a person.³⁷ Wallace consulted with advocates on the bill draft to make sure it addressed concerns about the system. The bill requires NYSED to commission a study on the following issues: the privacy implications of collecting sensitive biometric information; the risks of false identification for certain subgroups of individuals; whether information from the system might be shared with outside individuals, including law enforcement; the length of time information from the system can be retained; the risk of an unauthorized breach; maintenance costs; audits of the vendors; and how the technology should be disclosed to the public.³⁸ These questions are critical for analyzing the utility, efficacy, and harms of such systems, as is involving the public in decisions relating to the use of surveillance technology in schools.

2 The bill requires NYSED to consult with many New York State agencies in preparing the report and requires the Commissioner of Education to hold public hearings seeking feedback from teachers, school administrators, parents, and experts in school safety, data privacy, and civil rights and civil liberties.³⁹ In many ways, Wallace’s bill mirrors the concerns raised by residents in the community and advocates across the state and country. A senate version of the bill was introduced in April 2019.⁴⁰ The bill passed the New York Assembly with a bipartisan vote of 128 to 19 on the final day of the 2019 legislative session.⁴¹ The bill was not considered in the Senate, effectively killing the bill for the 2019 legislative session and teeing up a new fight in 2020.

3 Meanwhile, the community continued its efforts to prevent the use of the technology. Connor Hoffman, a reporter from the *Lockport Journal*, attended every school board meeting and filed multiple requests for information from the school district and NYSED. Hoffman received information that had not yet been publicly disclosed about the accuracy rates of Lockport’s system, revealing that Black women are sixteen times as likely as white men to be misidentified by the system.⁴² The persistent reporting led to national press coverage, including a feature in the *New York Times*,⁴³ a *New York Times* op-ed by Shultz,⁴⁴ and an MTV News documentary.⁴⁵ Without the diligence of concerned citizens and the local and national press, Lockport’s acquisition of the facial recognition system and NYSED’s failure to regulate this type of technology might have gone unnoticed.

36 Sup., note 16.

37 Ibid.

38 Ibid.

39 Ibid.

40 Senate Bill S5140-B, <https://www.nysenate.gov/legislation/bills/2019/s5140>. Introduced by Senator Brian Kavanagh, a senator representing New York’s 26th Senate District, which includes Lower Manhattan and parts of Brooklyn.

41 New York State Assembly, A06787 Floor Votes, https://assembly.state.ny.us/leg/?default_fld=&bn=A06787&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y.

42 *New York Civil Liberties Union v. New York State Education Department*, Index No. 903807-20, Exh. 9, G-2, p. 94, Albany County Supreme Court, June 18, 2020.

43 Davey Alba, “Facial Recognition Moves into a New Front: Schools,” *New York Times*, February 6, 2020, <https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html>.

44 Jim Shultz, “Opinion: Spying on Children Won’t Keep Them Safe,” *New York Times*, June 7, 2019, <https://www.nytimes.com/2019/06/07/opinion/lockport-facial-recognition-schools.html>.

45 MTV News (@MTVNEWS), “.@NYCLU says tech companies are using the fear of school shootings to turn students into lab rats for experimental technology. Meet the 25-year-old reporter @_hoffingtonpost who’s exposing the spread of facial recognition in schools,” Twitter, March 12, 2020, 12:31 p.m., <https://twitter.com/MTVNEWS/status/1238140444992774145>.

Despite the pushback, Lockport activated its facial recognition system on January 2, 2020.⁴⁶ Parents and students were not notified ahead of the deployment, nor were they given a chance to publicly comment on the system.⁴⁷ It remains unclear why the district pushed ahead with the system given the concerns of the community.

Despite this setback, there have been promising developments in the community's fight against this technology. Though the 2020 legislative session was interrupted by the COVID-19 global pandemic, the bill was amended in both houses to increase the amount of time for the moratorium until July 2022 or until the Commissioner of Education explicitly authorizes the use of the technology after issuance of the report, whichever occurs later.⁴⁸ The bill has widespread support from across the state and across the country, even garnering support from the United Federation of Teachers (UFT), the New York City affiliate of the American Federation of Teachers.⁴⁹ During the week of July 20, 2020, the bill passed both the Assembly and the Senate, and now awaits signature by the Governor to become law.⁵⁰

In February 2020, the New York Civil Liberties Union led a town hall in Lockport attended by nearly fifty parents and concerned community members about the system. The town hall was headlined by Shultz and a recent alumna of the school district.⁵¹ For many, it was the first time they had all been in a room together to discuss the system. Several people asked the school board members in attendance why there had not been a community forum sponsored by the district to answer questions and hear concerns. Community members expressed consternation over Lockport's lack of responsiveness, but planned to continue vocalizing their opposition and making their voices heard at school board meetings.⁵²

THE IMPORTANCE OF COMMUNITY-DRIVEN POLICY ADVOCACY

The community-driven advocacy response in Lockport demonstrates that persistent and organized public scrutiny can illuminate bureaucratic failures, shape necessary reforms, and shift narratives. The district's decision to purchase and use a facial recognition system follows a

46 See Troy Licastro, "Lockport City School District Begins Using Facial Recognition System," WIVB-TV, January 2, 2020, <https://www.wivb.com/news/local-news/niagara-county/lockport/lockport-city-school-district-begins-using-facial-recognition-system/>. Lockport deployed its system after receiving permission from NYSED. See also Temitope Akinyemi to Michelle Bradley, <https://int.nyt.com/data/documenthelper/6688-nysed-lockport/03fc55526445f8ef41aa/optimized/full.pdf>.

47 "Something this big should have been properly told to us," Christianna Silva, "Facial Recognition Technology Is Taking Over Schools—and Students Aren't OK with It," *MTV News*, March 13, 2020, <http://www.mtv.com/news/3159161/facial-recognition-technology-schools-students-respond/>.

48 Sup., note 16.

49 This is the same organization that experimented with Clearview AI's technology. See Michael Elsen-Rooney, "Racial Justice Groups Criticize City Teachers Union's Use of Controversial Face Recognition Technology," *Daily News*, March 27, 2020, <https://www.nydailynews.com/new-york/education/ny-uft-facial-recognition-20200327-msxxn5mmw5dtjmrjsfjy7xqq-story.html>.

50 New York Assembly Bill A6787-D, <https://www.nysenate.gov/legislation/bills/2019/a6787>.

51 Connor Hoffman, "Spotlight on Facial Recognition: Civil Liberties Union Hosts a 'Town Hall' in Lockport," *Lockport Union-Sun & Journal*, February 25, 2020, https://www.lockportjournal.com/news/local-news/spotlight-on-facial-recognition-civil-liberties-union-hosts-a-town/article_32c29556-9f05-5934-8c03-29ef5e08212a.html.

52 In addition to concerns over the use of the facial recognition system, community members demanded that a beloved middle-school peer mediator's employment not be terminated by the school district. Connor Hoffman, "Trying to Have Mr. Cheatham's Back," *Lockport Union-Sun & Journal*, January 23, 2020, https://www.lockportjournal.com/news/trying-to-have-mr-cheatham-s-back/article_a814300a-3e61-11ea-b6fa-43627916ccc3.html.

common yet flawed pattern that government officials rely on to justify the adoption of surveillance technologies. The school district conflated an abstract or speculative risk to student safety with an objective fact of real harm. They installed an unproven and potentially ineffective system that will likely undermine students' civil rights and liberties. Though school safety concerns are legitimate and warrant critical review, the school district's actions demonstrated the inherently political nature of privileging certain risks and interests over community needs.⁵³ Rather than consult the community to assess actual needs and concerns, the district adopted a technological solution in search of a problem.

The community-driven advocacy made the flawed logic of this approach apparent. Parents shifted the discourse from debating whether the biometric surveillance system was necessary to focusing on the real harms posed to students if the school district decided to move forward against community opposition. In particular, Shultz's early writings on the facial recognition system emphasized the dangers to student and teacher privacy at a time when the district trivialized the idea that the system could negatively impact student privacy.⁵⁴ In 2019, however, the superintendent of the school district reluctantly acknowledged that "[p]rivacy matters are a big deal nowadays."⁵⁵ This emphasis on privacy is echoed in the current legislation.⁵⁶

Lockport also failed to acknowledge that deployment of a flawed facial recognition system could compound preexisting racial-equity concerns regarding its school safety practices and policies. For instance, the district has struggled to address existing issues of disproportionate discipline when it comes to students of color, a problem that can be exacerbated by the use of an inaccurate and racially biased facial recognition system.⁵⁷

During Lockport's school board elections this year, a new slate of parents, energized by the fight against facial recognition technology, organized to run for multiple open seats on the board.⁵⁸ This year's voter turnout was four times higher than the district's five-year average turnout.⁵⁹ Though the fight in Lockport and New York State continues, this community-driven advocacy effort demonstrates the importance of empowering those directly affected by problematic government decision-making to lead the change they want to see.

53 See Hope, "Seductions of Risk," in *Schools Under Surveillance*, for a discussion of how adoption of surveillance technologies can unreasonably limit students' educational experience. See also Mary Douglas and Aaron Wildavsky, *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers* (Berkeley: University of California Press, 1983), 29–38. Douglas and Wildavsky describe how labeling risks is a social process complicated by new technologies that provoke cultural and social reassessments.

54 Sup., note 31: "When the privacy issue was raised at that March meeting it was dismissed away as a joke about the likelihood of North Korea hacking into student records."

55 Connor Hoffman, "Lockport School District Cancels Security Contract," Lockport Union-Sun & Journal, April 11, 2019, https://www.lockportjournal.com/news/local_news/lockport-school-district-cancels-security-contract/article_b5612839-211e-53ff-a70b-c1de1f66abd6.html.

56 Sup., note 16. The legislation requires NYSED to consider "the privacy implications of collecting, storing, and/or sharing biometric information of students, teachers, school personnel and the general public entering a school or school grounds."

57 During the 2015–2016 school year, Black students made up just 12.3 percent of the student population but represented more than a quarter of the students receiving out-of-school suspensions. Students of two or more races represented 5.9 percent of the student population in Lockport, but 15 percent of the students who received out-of-school suspensions. See Civil Rights Data Collection, "Lockport City School District," 2015, <https://ocrdata.ed.gov/Page?t=d&eid=31160&syk=8&pid=2539&Report=6>. See also Paul Hirschfield, "School Surveillance in America: Disparate and Unequal," in *Schools Under Surveillance*, for a description of the disparate impact of school surveillance.

58 Jim Shultz, "Time for Change on the Lockport School Board," Lockport Union-Sun & Journal, May 23, 2020, https://www.lockportjournal.com/opinion/jim-shultz-time-for-change-on-the-lockport-school-board/article_142c3905-0612-54d6-8f66-22097b35e5cb.html.

59 Connor Hoffman, "Renee Cheatham wins a seat on the school board," Lockport Union-Sun & Journal, June 18, 2020, https://www.lockportjournal.com/news/local_news/renee-cheatham-wins-a-seat-on-the-school-board/article_6e3e73ba-b42c-5820-98df-01ccd23d234a.html.

AINOW¹