3

FRT in ‘Bloom’

Beyond Single Origin Narratives

Simon Michael Taylor

3.1 INTRODUCTION

On 10 September 2020, Pace Gallery in London held an exhibition by the artist Trevor Paglen examining the visual products from artificial intelligence and digital data systems.[1] Titled ‘Bloom’, the exhibition featured an over-sized sculpture of a human head. Bald, white, and possibly male, this eerily symmetrical ‘standard head’ had been modelled on measurements from canonical experiments in facial recognition history by Woody Wilson Bledsoe, Charles Bisson, and Helen Chan Wolf occuring at Panoramic Research Laboratory in 1964.[2]

Centring this ‘standard head’ in the space, Paglen surrounded it with photographic prints of leaves and flowers re-composed from RAW camera files by computer vision algorithms. These machine visualisations of nature encircled the ‘standard head’ illustrating how digital imaging using autonomous toolsets can achieve significantly different graphical outcomes. The exhibit foregrounded face recognition technology yet provoked viewers to consider the cross-practice connections between computing and data classification, humans and nature, and how image-making is becoming technically autonomous.[3] Another take-away is how these systems require

The author would like to acknowledge Stephanie Dick, Ausma Bernotaite, and Kalervo Gulson for their generous insight on different case-studies that comprise this chapter. Thanks also to Monika Zalneirute and Rita Matulionyte for their editorial guidance, and finally, Kathryn Henne at Australian National University, School of Regulation and Global Governance for her continued support.

[1] Trevor Paglen, ‘Bloom’, Pace Gallery (10 September–4 November 2020).

[2] Paglen obtained the dataset and visual materials on Bledsoe’s experiments from correspondence with Harvard trained historian of technology Stephanie Dick and her research at the Briscoe Center for American History, University of Texas. See Bledsoe, Woodrow Wilson, and Helen Chan. “A man-machine facial recognition system—some preliminary results.” Panoramic Research, Inc, Technical Report PRI A 19 (1965), Palo Alto, California.

[3] Paglen states that ‘sophisticated machine learning algorithms that classify and categorise people are incentivized by assumptions of a stable relationship between the image and its measurement – but there are usually bad politics attached [and a misapprehension that these are human ways of seeing and of comprehending]’; Camille Sojit Pejcha, ‘Trevor Paglen wants you to stop seeing like a human’ (15 September 2020), *Document*, www.documentjournal.com/2020/09/trevor-paglen-wants-you-to-stop-seeing-like-a-human/.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

multi-faceted elements to work and the 'mushrooming and blossoming from all kinds of datasets'.[4]

As a form of networked visual surveillance, facial recognition technology (FRT) works from the extent to which it operates in larger information infrastructures, FRT 'is not a single technology but an umbrella term for a set of technologies'.[5] These digitally networked systems allow imaging data to transform from one state to another, and transfer from one site to another. Recent improvements in FRT, as a remote identification system, has reached a point to be technically possible to capture biometric images and data from subjects in public, private, and personal spaces, or interactions online, without their consent or awareness, or adequate regulatory oversight. This includes a distribution of sensitive and personal user information between state and private-sector organisations, while contributing to training machine learning tools using honeypots of data, and enabling 'ever more sophisticated and effective forms of social control'.[6]

Unlike the suggestion of Paglen's exhibition, the origins of FRT cannot be reduced to the experiments in 1964. We need to widen the lens as the technical operations Stakeholders inside these systems are globally distributed and as Chair of Electronic Frontiers Australia's Policy Committee, Angus Murray iterated require 'bargains of trust'.[7] For example, Domestic and federal police agencies use systems that rely on huge amounts of data aggregation in private cloud servers and proprietary hardware that store and transmit data from online platforms, smart devices, foreign owned closed-circuit television (CCTV) companies and creators of wearable body cameras.[8] In Australia, retail outlets such as Bunnings use FRT and identity data to extract information from social media, where most people have images of themselves uploaded. They perform analysis based on the specific visits and transactions for certain shoppers.[9] Similarly images captured in public spaces, of crowds or of protesters, can be matched to social media posts or online forums managed by global technology firms, such as Facebook and Google, or transnational intelligence agencies such as

[4] David Gershgorn, 'The data that transformed AI research – And possibly the world' (26 July 2017), Quartz, https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world. Noted by Fei-Fei Li (the creator of the machine learning database Image-Net). For use of machine learning systems on Image Net, see E. Denton, A. Hanna, R. Amironesei, A. Smart, and H. Nicole, 'On the genealogy of machine learning datasets: A critical history of ImageNet' (2021) 8(2) *Big Data & Society*, https://doi.org/10.1177/20539517211035955.

[5] Nikki Stevens and Os Keyes, 'Seeing infrastructure: Race, facial recognition and the politics of data' (2021) 35(4–5) *Cultural Studies* 833–853, at 833.

[6] Kelly A. Gates, 'Introduction: Experimenting with the face' in *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, 2011), p. 5.

[7] 'Expert Panel: AI, Facial Recognition Terchnology and Law Enforcement' hosted by AUSCL Australasian Society for Computers + Law, May 5th 2022.

[8] Katelyn Ringrose, 'Law enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns' (2019) 105 *Virginia Law Review Online* 57–66.

[9] Dennis Desmond, 'Bunnings, Kmart and The Good Guys say they use facial recognition for "loss prevention". An expert explains what it might mean for you' (15 June 2022), *The Conversation*, https://theconversation.com/bunnings-kmart-and-the-good-guys-say-they-use-facial-recognition-for-loss-prevention-an-expert-explains-what-it-might-mean-for-you-185126.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

the NSA and GCHQ. In the United Kingdom, Daragh Murray witnessed FRT software draw rectangles around the faces of people in public streets from a live CCTV feed. The system then extracted key features and compared these with stored features of criminal suspects in a watch list.[10] Matching an image to a watchlist is not the only function to consider here, but a need to query the distribution and ownership of data in the system being collectively assembled by the Tokyo-based technology giant NEC, in the example provided above.[11] Other examples of this diffuse and operational data flow include how China's Zhejiang Dahua Technology Co. Ltd sold thermal imaging cameras, armed with facial recognition software, to scan workers entering Amazon factories during COVID-19, that is despite them being black-trade listed in the United States.[12]

FRT and its computer procedures are therefore systems and 'technologies in the making', not artefacts with singularly defined origins and easy to regulate outcomes.[13] While an abundance of research looks at the use of FRT in border security and biometric surveillance,[14] retail shopping or school aged education,[15] and the gendering and racial divide between datasets with calls to ban these systems,[16] other elements also require scholarly, legislative, and regulatory attention.

[10] Pete Fussey and Daragh Murray, 'Independent report on the London Metropolitan Police service's trial of live facial recognition technology' (July 2019), University of Essex Repository, https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf; see also Davide Castelvecchi, 'Is facial recognition too biased to be let loose?' (2020) *Nature* 587 347–349.

[11] NEC, 'A brief history of facial recognition' (12 May 2020), *NEC Publications and Media*, www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/.

[12] China's Zhejiang Dahua Technology Co Ltd shipped 1,500 cameras to Amazon in a deal valued at close to $10 million – see Krystal Hu and Jeffrey Dastin, 'Exclusive: Amazon turns to Chinese firm on U.S. blacklist to meet thermal camera needs' (4 April 2020), *Reuters*, www.reuters.com/article/ushealth-coronavirus-amazon-com-cameras/exclusive-amazon-turns-to-chinese-firm-on-u-s-blacklist-tomeet-thermal-camera-needs-idUSKBN22B1AL?il=0. For the black-listing of Dahua, see US Department of Commerce, 'U.S. Department of Commerce adds 28 Chinese organisations to its entity list', Office of Public Affairs, Press Release (7 October 2019), https://2017-2021.commerce.gov/news/press-releases/2019/10/us-department-commerce-adds-28-chinese-organizations-its-entity-list.html

[13] This is needed as a corrective to those who focus uncritically on such things as 'the computer and its social impacts but then fail to look behind technical things to notice the social circumstances of their development, deployment, and use'. Langdon Winner, 'Do artifacts have politics?' (1908) 109(1) *Daedalus* 121–136, at 112.

[14] Lucas D. Introna and David Wood, 'Picturing algorithmic surveillance: The politics of facial recognition systems' (2004) 2(2/3) *Surveillance & Society* 177–198; Lucas D. Introna, 'Disclosive ethics and information technology: Disclosing facial recognition systems' (2005) 7(2) *Ethics and Information Technology* 75–86; Lucas D. Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (Center for Catastrophe Preparedness and Response, New York University, 2010), pp. 1–60.

[15] Mark Andrejevic and Neil Selwyn, *Facial Recognition* (John Wiley & Sons, 2022).

[16] Luke Stark, 'Facial recognition is the plutonium of AI' (2019) 25(3)*XRDS: Crossroads, The ACM Magazine for Students* 50–55; Richard Van Noorden, 'The ethical questions that haunt facial-recognition research' (2020) 587 *Nature* 354–358. Joy Buolamwini and Timrit Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) 81 *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, in Proceedings*

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

This chapter considers how large-scale technical systems such as FRT have *bloomed* yet build on the echnical roots of multiple systems and the provenance of data sources that remain under considered. Tracing the genealogical origins and provenance of such datasets and statistical toolsets plays an important role in framing current uses for regulatory challenges. In this regard, this chapter presents empirical findings from research on early Indian statistical measures, the convergence of Chinese and Western technology companies, and the increase in computer vision experiments including those conducted on animals for bio security identification purposes. This chapter argues these diverse material innovations and information domains not only act as testbeds for FRT systems, but encompass some of the globalised products contained in FRT infrastructure.[17]

3.2 FRT DOES NOT HAVE A SINGULAR ORIGIN, THEY ARE 'SYSTEMS IN MOTION'

Bledsoe's 'standard head' algorithm didn't remain at the University of Texas nor in the domain of artificial intelligence history. Owing to funding by the RAND Corporation, the algorithm worked its way into informational models for law enforcement purposes. In the development of the New York State Intelligence and Identification System (NYSIIS), Bledsoe was recruited to develop his algorithm to computationally solve 'the mug-file problem'.[18] By contributing to the world's first computerised criminal-justice information-sharing system,[19] as Stephanie Dick posits, Bledsoe's algorithm and its ideas *travelled* with his over-simplifications and data assumptions in tow.[20] This

of Machine Learning Research 77–91; Jacqueline Cavazos, Jonathon Phillips, Carlos Castillo, and Alice O'Toole, 'Accuracy comparison across face recognition algorithms: Where are we on measuring race bias?' (2019) 3(1) *IEEE Transactions on Biometrics, Behavior, and Identity Science* 101–111; Morgan Scheuerman, Kandrea Wade, Caitlin Lustig, and Jed R. Brubaker, 'How we've taught algorithms to see identity: Constructing race and gender in image databases for facial analysis' (2020) 4(CSCW1) *Proceedings of the ACM on Human-Computer Interaction* 1–35.

[17] A main debate is whether this process should be considered a 'diffusion' from an established centre, such as Beldsoe's laboratory, or a more globalised network of exchanges. This changes the way these systems can be understood, explained, and regulated. Decentred histories give attention to members of other classes, such as the experiences of women, exploitation of Indigenous groups, and non-humans including animals. They include histories from parts of the world outside the United States and Europe. See Eden Medina, 'Forensic identification in the aftermath of human rights crimes in Chile: A decentered computer history' (2018) 59(4) *Technology and Culture* S100–S133; Erik Van der Vleuten, 'Toward a transnational history of technology: Meanings, promises, pitfalls' (2008) 49(4) *Technology and Culture* 974–994.

[18] Ben Rhodes, Kenneth Laughery, James Bargainer, James Townes, and George Batten, Jr, 'Final report on phase one of the Project "A man-computer system for solution of the mug file problem"' (26 August 1976), Prepared for the Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement, and Criminal Justice, under Grate 74-NI-99-0023 G.

[19] Jeffrey Silbert, 'The world's first computerized criminal-justice information-sharing system, the New York State Identification and Intelligence System (NYSIIS)' (1970) 8(2) *Criminology* 107–128.

[20] Stephanie Dick, 'The standard head' in Gerardo Con Diaz and Jeffrey Yost (eds.), *Just Code!* (Johns Hopkins University Press, 2024).

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

influenced not only law enforcement databases and decisions on criminal targets in the United States, but also FRT developments that followed.[21] In its final state the algorithm was not used to automatically detect faces – as FRT does now – but contributed to a standardisation of 'mug shot' photos for computer filing systems. Bledsoe, who was later the president of the Association for the Advancement of Artificial Intelligence, used 2,000 images of police mug shots as his 'database' for making comparisons with a new set of photographs to detect any similarity. This American National Standards Institute Database, whose archives of mug shots featured convicted criminals (and those just accused), was the predominant source of visual information for Bledsoe's facial-recognition technology (a role now filled by social media).[22] To this end, Bledsoe and his Panoramic Research collaborators manually drew over human facial features with a device that resembled an iPad called a GRAFACON or RAND tablet. By using a stylus, images were rotated and re-drawn onto the tablet and recorded as coordinates on a grid. This produced a relatively high-resolution computer readable image. A list of distances were calculated and recorded as a *person's identification code* for locations such as the mouth, nose, or eyes.[23] Facial recognition (at this time) was a mathematical code of distances between features, drastically reducing individual and social nuances between them, and largely informed by Bayesian decision theory to use '22 measurements to make an educated guess about the whole'.[24]

In essence, Bledsoe had computerised the mug shot into a 'fully automated Bertillon system for the face'.[25] This system, invented by French criminologists Cesare Lombroso and Alphonse Bertillon in 1879, gained wide acceptance as a reliable and scientific method for criminal investigation, despite problematic eighteenth-century anthropometric experiments. The mug shot was invented to

[21] See A. Jay Goldstein, Leon D. Harmon, and Ann B. Lesk, 'Identification of human faces' (1971) 59(5) *Proceedings of the IEEE* 748–760; also Takeo Kanade, 'Picture processing by computer complex and recognition of human faces' (1973), PhD thesis, Kyoto University; and finally, the development of Principle Component Analysis – a compression of facial data that allowed for faster computer comparisons to be made (crucial to automation). Lawrence Sirovich and Michael Kirby, 'Low-dimensional procedure for the characterization of human faces' (1987) 4(3) *Josa a* 519–524.

[22] In other words, original facial-recognition software was built from images of prisoners repurposed by the US government without their consent. Trevor Paglen produced another artistic work on this - 'They Took the Faces from the Accused and the Dead …(SD18)', 2020, the artist and Altman Siegel, San Francisco. For how these databases are constructed and configured see Craig Watson and Patricia Flanagan, 'NIST special database 18: Mugshot identification database' (April 2016), Information Technology Laboratory, National Institute of Standards and Technology, www.nist.gov/system/files/documents/2021/12/06/readme_sd18.pdf.

[23] By producing a tape that could be fed to another, more powerful computer, the distance between specific points on the face then became a 'coded definition of that face'. Dick, 'The standard head'.

[24] For a biographical narrative of Bledsoe's efforts with Panoramic Research see Shaun Raviv, 'The secret history of facial recognition' (21 January 2020), *Wired*, www.wired.com/story/secret-history-facial-recognition/.

[25] As Aradau and Blanke argue, controlling error in these systems requires repeated measurements and often converge towards' the average'. This becomes the 'standard' benchmark with which to measure and render individuals uniquely identifiable. Claudia Aradau and Tobias Blanke, 'Algorithmic surveillance and the political life of error' (2021) 2(1) *Journal for the History of Knowledge* 1–13, at 5.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

recognise criminal suspects who were repeatedly arrested: portraits were drawn and statistically labelled on common morphological characteristics.[26] The resulted 'mug shots' were standardised and collected by police departments and accepted as evidence in courts. Photo IDs modelled on the mug shot not only became an official format for policing, but have become standard issue in nation-state passports presented at airports and for driver's licence photographs. The first ever US photo driver's licence, issued in 1958, was created by French security company IDEMIA – a world leader in biometric security. Founded in 1922 as the defence contractor SAGEM, it then became SAGEM-Morpho in the 1980s, and parts of IDEMIA go back even further, and they have effectively led to every shift in the photo identity issuance and credentialling in the US since.[27]

Bledsoe's 1960s laboratory experiments thus relied on two separate building blocks invented in France. Hampered by the technology of his era, Bledsoe's ideas for FRT were not truly operationalised until the 1990s – driven by a technological wave of mobile phone and personal computer sales, online networked wireless video systems, and digital cameras.[28] Yet the experimental use of FRT is still being conducted in a way largely never done before.[29] Clare Garvie contends that forms of automated imaging for policing actions remain unregulated and represent a 'forensic science without rules':

> [T]here are no rules when it comes to what images police can submit to facial recognition [databases] and algorithms to help generate investigative leads. As a consequence, agencies across the country can, and do, submit all manner of probe photos – low-quality surveillance camera stills, social media photos with filtering, and scanned photo album pictures. Records from police departments show they may also include computer-generated 3D facial features, or composite and artistic sketches.[30]

[26] From vast literature on Bertillon, refer to Jonathan Finn, *Capturing the Criminal Image: From Mug Shot to Surveillance Society* (University of Minnesota Press, 2009); Keith Breckenridge, *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present* (Cambridge University Press, 2014).

[27] This also included the first automated fingerprint system for the FBI, building contactless scanners, and the launch of electronic ID (eID) in the United States in 2017. See IDEMIA, 'Innovation wall: A history of expertise' (2022), www.idemia.com/wp-content/uploads/2021/01/idemia-history-of-expertise.pdf; and see FindBiometrics, 'IDEMIA's Matt Thompson on the reality of mobile ID and "Identity on the Edge"'(4 May 2021), Interview at Find Biometrics: Global Identity Management, https://findbiometrics.com/interview-idemia-matt-thompson-mobile-id-identity-on-the-edge-705059/.

[28] For an analysis of 'smart photography' and facial recognition see Sarah Kember, 'Face recognition and the emergence of smart photography' (2014) 13(2) *Journal of Visual Culture* 182–199. The use of digital photography also challenges 'how can the photographic image continue to "guarantee" the existence of reality in what it shows when pixel by pixel manipulation allows a seamless modification?' Scott McQuire, 'Digital photography and the operational archive' in Sean Cubitt, Daniel Palmer, and Nathaniel Tkacz (eds.), *Digital Light* (Open Humanities Press, 2015), chapter 6 (pp. 122–143), at p. 142.

[29] Clare Garvie, 'Garbage in, garbage out: Face recognition on flawed data' (16 May 2019), Georgetown Law, Center on Privacy & Technology, www.flawedfacedata.com/.

[30] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, 'The perpetual line-up: Unregulated police face recognition in America' (18 October 2016), Georgetown Law, Center on Privacy & Technology, www.perpetuallineup.org.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

In the next section, I explore how the automation of FRT relies not only on a diverse manufacturing of 'images' – products of reduction, appropriation, transformation, or digital manipulation – and situated instances of exploitation conducted in South America, the United States, France, Russia, Japan, and China to name a few different jurisdictions, but also how modern FRT resurrects a century old vision of 'statistical surveillance'.[31] To do so, I consider how a 100 year old mathematical experiment in British India has aided the probabilistic functionality of autonomous FRT systems.

3.3 THE 'MIND BOGGLING SYSTEMS' WHERE EVERYONE ONLY EVER HAS ONE ID

In 1991 Turk and Pentland produced the first real-time automated face recognition.[32] Famously, this was deployed at the crowded USA Super Bowl in 2001. This experimental trial was called 'Facefinder'. The system captured surveillance images of the crowd and compared them with a database of digital mug shots held by Tampa police, the Florida Department of Law Enforcement and the FBI.[33] The experiment not only demonstrated the potential for remote surveillance of crowds, but also led to the National Institute of Standards creating a Face Recognition Vendor Test (FRVT) to evaluate this emerging FRT market.

A quick look at the ongoing FRVT of 1: N facial algorithms reveals a globalised picture: 'The report lists accuracy results alongside developer names as a useful comparison of facial recognition algorithms and assessment of absolute capability. The developer totals constitute a substantial majority of the face recognition industry.'[34] This includes performance figures for 203 prototype algorithms from the research laboratories of over fifty commercial developers and one university. Similar to Beldsoe's 1960s experiments for NYSIIS, this evaluative test scenario also uses

[31] Oscar H. Gandy, 'Statistical surveillance: Remote sensing in the digital age' in Kevin Haggerty, Kirstie Ball, and David Lyon (eds.), *Routledge Handbook of Surveillance Studies* (Taylor & Francis, 2012), pp. 125–132.

[32] The approach used a process to break down human faces into principle components via statistical means and these became 'standardised ingredients' known as eigenfaces. The experiment was constrained by environmental factors, but created significant interest in automated face recognition. M. Turk and A. Pentland, 'Eigenfaces for recognition' (1991) 3(1) *Journal of Cognitive Neuroscience* 71–86.

[33] At the Super Bowl signs advised fans that they were under video surveillance. The system identified nineteen people – all petty criminals. No one was detained or questioned because Facefinder was an experiment. See Vicky Chachere, 'Biometrics used to detect criminals at Super Bowl' (13 February 2001), *ABC News*, https://abcnews.go.com/Technology/story?id=98871&page=1.

[34] Patrick J. Grother, Mei L. Ngan, and Kayee K. Hanaoka, 'Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification' (November 2018), NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.IR.8238. The primary dataset is comprised of 26.6 million reasonably well-controlled live portrait photos of 12.3 million individuals. Three smaller datasets contain more unconstrained photos: 3.2 million webcam images, 200,000 side-view images, and 2.5 million photojournalism and amateur photographer photos. These datasets are sequestered at NIST, meaning that developers do not have access to them for training or testing.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

frontal mug shots and profile view mug shots alongside desktop webcam photos, visa application photos, immigration lane photos, and traveller kiosk photos.

A brief survey of this report illustrates the scale and scope of a global FRT market. To name a few vendors, the developers and their places of origin include NEC (Tokyo); Microsoft (United States); Veritas (Spain); Herta Security (Spain); AnyVision (Israel); IDEMIA (France), utilised in Kenya and in Turkey; Daon (Ireland); Dahua (China); Moonwalk (China); Sensetime (China); Hyperverge (California); Cognitec (Germany); QNAP (Taiwan); Tevian (Russia); VisionLabs (Russia/Netherlands); Clearview AI (United States); DeepGlint (China) and finally Neurotechnology (Lithuania), which is a provider of deep-learning-based solutions for high-precision biometric identification and object recognition technology.

Importantly, the Lithuania based Neurotechnology recently partnered with Tata Consultancy Services as one of three biometric service providers for the largest biometric ID system in the world, Aadhaar.[35] Co-ordinated by The Unique Identification Authority of India, the system registers people and compares their facial biometric with the existing records of 1.3 billion people to verify applicants have not registered under a different name. Aadhaar is 'a mind-boggling system', says Anil Jain, a computer scientist who consulted on the scheme, 'and the beauty is that it ensures one person has only one ID'.[36]

India has a rich history of producing material and statistical innovations to identify individuals based on their physical characteristics.[37] In 2020, Google posted an online tribute to Professor Prasanta Chandra Mahalanobis (1893–1972) as part of its 'Arts and Culture' series.[38] Mahalanobis is famous for creating new statistical and biometric functions as key technologies he advocated to the world through his Indian Statistical Institute.[39] The global celebration of his work was recognised in part after his creation of a similarity distance metric in 1936. This was produced from his specific interest in

[35] Neurotechnology, 'Neurotechnology and TCS selected by UIDAI to provide biometric de-duplication and authentication for India's Aadhaar ID program', Neurotechnology Press Release (22 March 2021), www.neurotechnology.com/press_release_india_uidai_aadhaar_id.html.

[36] For references on Aadhaar, see Bidisha Chaudhuri and Lion König, 'The Aadhaar scheme: A cornerstone of a new citizenship regime in India?' (2018) 26(2) *Contemporary South Asia* 127–142; Amiya Bhatia and Jacqueline Bhabha, 'India's Aadhaar scheme and the promise of inclusive social protection' (2017) 45(1) *Oxford Development Studies* 64–79; Kalyani Menon Sen, 'Aadhaar: Wrong number, or Big Brother calling' (2015) 11(1) *Socio-Legal Review* 85–108.

[37] See Keith Breckenridge, *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present* (Cambridge University Press, 2014). Chapter 3 (pp. 90–114), titled 'Gandhi's biometric entanglement: Fingerprints, satyagraha and the global politics of Hind Swaraj', perfectly captures the complexity when dealing with the question of biometrics, and a mobility in their use.

[38] Indian Statistical Institute, 'Father of Indian statistics: Prof. Prasanta Chandra Mahalanobis' (2020), Google Arts and Culture, https://artsandculture.google.com/exhibit/father-of-indian-statistics-prof-prasanta-chandra-mahalanobis%C2%A0/0AISK23-669lLA.

[39] Prasanta Chandra Mahalanobis, 'Statistics as a key technology' (1965) 19(2) *The American Statistician* 43–46; and refer to Paidipaty Poornima, 'Testing measures: Decolonization and economic power in 1960s India' (2020) 52(3) *History of Political Economy* 473–497.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

racial classification.[40] He developed a biometric function to analyse and identify people based on physical and racial similarity. To do so he compared data collected from the Chittagong Hill Tract area (modern Bangladesh) with international race data sets collected from Swedish and Chinese records.[41] He then set about learning how to create an identification of race based on statistical measurements of facial features and their similarity, which he could apply in India. The aim was to help identify exotic and ethnic caste groups to be classified in the British colonial administration.[42]

Significantly, he also innovated by using facial photographs of living subjects to compare the accuracy of his biometric measurements, compared with analysing skulls in the era's practice of phrenology.[43] By testing his distance function with the invention of an experimental imaging device in 1937, Mahalanobis was a central figure in pushing 'part of a biometric nationalism in which the face provided a form of data'.[44] His metric, commonly known as a Mahalanobis Distance Function, despite being created eighty-six years ago, is consistently used in modern FRT.

Even the most sophisticated and large-scale FRT systems necessitate this basic approach of comparing images on facial features by using scores that compare a match of the similarity.[45]

In technical terms, the selection of a decision metric – such as the Mahalanobis Distance Function – '[h]elps to measure distances between specific facial features and generate a unique representation (as a 'facial signature') for each human face.[46] Similar to Bledsoe's code, this is then compared with a database of stored images in order to match a face to similar images.

In this regard, similarity measure functions operationalise the matching process as a critical decision-making module. Selection of the proper similarity measure is thus

[40] Dasgupta Somesh, 'The evolution of the D statistic of Mahalanobis' (1993) 55(3) *Sankhyā: The Indian Journal of Statistics, Series A (1961–2002)* 442–459; Prasanta Chandra Mahalanobis, 'On the generalized distance in statistics' (1936) 12 *Proceedings of the National Institute of Science India* 49–55.

[41] Simon Michael Taylor, Kalervo N. Gulson, and Duncan McDuie-Ra, 'Artificial intelligence from colonial India: Race, statistics, and facial recognition in the Global South' (2021) 48(3) *Science, Technology, & Human Values*, https://doi.org/10.1177/01622439211060839.

[42] Somesh, 'The evolution of the D statistic', p. 448.

[43] Mahalanobis Prasanta Chandra, 'A new photographic apparatus for recording profiles of living persons' (1933) 20 *Proceedings of the Twentieth Indian Science Congress. Patna Secondary Anthropology* 413.

[44] Mukharji Projit Bihari, 'Profiling the profiloscope: Facialization of race technologies and the rise of biometric nationalism in inter-war British India' (2015) 31(4) *History and Technology* 376–396, at 392.

[45] This applies whether for connectionist approaches such as using neural networks or deep learning; or statistical based approaches using hidden Markov models; or biometric probes with template feature matching; or geometric approaches to frontal face recognition such as eigenface images or geometrical feature matching.

[46] Ada Lovelace Institute, 'Beyond face value: Public attitudes to facial recognition technology' (September 2019), Nuffield Foundation, Ada Lovelace Institute, London, p. 5, www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

an important determination for the accuracy of the matching result. Such measures include Minkowski distances, Mahalanobis distances, Hansdorff distances, Euclidean, and cosine-based distances.[47] Yet the Mahalanobis distance is the best at structuring data for unknown targets. This is critical to criminal subject investigations for matching suspects from surveillance images in supermarkets, stadiums, or of protest crowds. The similarity measure enables high-speed cluster analysis – critical to a speed of decision-making – especially for faces with a high-number of variables and in relation to fitting an unknown person into a known database. FRT can then determine if an unknown image (taken from a web profile or a surveillance camera) matches a person in the database (compared with drivers' licences or mug shots). This approach is also suitable for machine learning and is a prominent approach for training systems on person re-identification by 'improving classification through exploiting structures in the data'.[48]

As Adriana Dongus suggests, '[t]he large datasets produced by science and law enforcement at the turn of the nineteenth century continue to form the material backbone and precedent to current machine learning.'[49] By examining the critical and ubiquitous distribution and embedment of early decision classifiers, we establish the importance of selecting certain rule functions in 'a statistical layer' of FRT systems.

When applied to machine learning, this includes assigning weights to autonomously identify the importance in probable matches. This is used in image-labelled data sets,[50] to estimating facial position poses from video,[51] to automatically locating an unproductive worker on a factory floor,[52] or identifying ethnic minority faces in a crowd, as is occurring in China with the Uyghur (Uighur) population. While much important work on facial recognition is salient to the United States,[53] there is a need to examine

[47] Enrico Vezzetti and Federica Marcolin, *Similarity Measures for Face Recognition* (Bentham Science, 2015).

[48] The Mahalanobis distance function is ubiquitous owing to its algorithmic and biometric efficacy for structuring unknown datasets, its acceptability and incorporability into different decision systems, and the efficiency of being weighted to produce accurate results. See P. M. Roth, M. Hirzer, M. Köstinger, C. Beleznai, and H. Bischof, 'Mahalanobis distance learning for person re-identification' in S. Gong, M. Cristani, S. Yan, and C. C. Loy (eds.), *Person Re-Identification* (Springer, 2014), pp. 247–267.

[49] Machine learning tools often reuse elements that lie far afield from the scientific laboratories, statistical research institutes, and engineering settings in which they first took shape. See also Ariana Dongus, 'Galton's utopia – Data accumulation in biometric capitalism' (2019) 5 *Spheres: Journal for Digital Cultures* 1–16, at 11, http://spheres-journal.org/galtons-utopia-data-accumulation-in-biometric-capitalism/.

[50] Kate Crawford and Trevor Paglen, 'Excavating AI: The politics of images in machine learning training sets' (2021) 36(4) *AI & Society* 1105–1116.

[51] Shiming Xiang, Feiping Nie, and Changshui Zhang, 'Learning a Mahalanobis distance metric for data clustering and classification' (2008) 41(12) *Pattern Recognition* 3600–3612.

[52] Meredith Whittaker, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kaziunas, Varoon Mathur, Myers West, Rashida Richardson, Jason Schultz, and Oscar Schwartz, 'AI Now Report 2018' (2018), AI Now Institute.

[53] Cavazos et al., 'Accuracy comparison across face recognition algorithms'; Clare Garvie, 'Face recognition in US investigations: A forensic without the science' (5 August 2020), Webinar, UNSW Grand Challenges, online presentation, UNSW Sydney; Scheuerman et al., 'How we've taught algorithms to see identity'; Stark, 'Facial recognition is the plutonium of AI'.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

how FRT is conditioned on a globalised supply chain. This includes the 'production, schematization, maintenance, inflection, and reproduction of certain [decision] rules' and how they replicate use of problematic standards in public surveillance.[54]

Indeed, there has been a 'tendency to gloss over the amount of effort that goes into developing and integrating new technologies and systems with older technologies'.[55] Computation moves fast – yet many lessons remain and are yet to be learned.

From legislative, ethical, and regulatory standpoints, it is worth noting that biometric systems and data (including use of statistical functions and facial images) are constructed on complex and interoperable supply chains involving third-party vendors needed to make these systems work. Yet there is potential incentives built within these globalised computing systems to exploit regulatory gaps and vulnerabilities that could be used against various human populations at a later date.[56] The final section examines how Mahalanobis's 100 year old experiment is relevant not only to our digital identity systems today, such as the United Nations High Commission for Refugees (UNHCR) Population Registration and Identity Management Eco-System[57] but builds on different use-cases. These include not only nation-state surveillance, such as the identification and detection of ethnic minorities in China, but the increasing datafication of animals and computerisation of biosecurity measures in agriculture that can be transferrable to human populations.[58]

3.4 DYNAMIC MATCHING STRATEGIES IN FRT EXTEND BEYOND RECOGNISING HUMAN BEINGS

To securely identify forcibly displaced persons seeking UNHCR repatriation assistance at refugee processing centres the UNHCR records biometrics such as iris, fingerprints, and facial metrics.[59] Driven in part by a Biometric Matching Engine developed by Accenture, this Population Registration and Identity Management Eco-System (PRIMES) employs a patented 'dynamic matching strategy' comprising at least two sets of biometric modalities.[60] With the advent of new, technologically

[54] Alexander Monea and Jeremy Packer, 'Media genealogy and the politics of archaeology' (2016) 10 *International Journal of Communication* 3141–3159, at 3144.

[55] Gates, 'Introduction', p. 11.

[56] Caroline Compton, Fleur E. Johns, Lyria Bennett Moses, Monika Zalnieriute, Guy S. Goodwin-Gill, and Jane, McAdam, 'Submission to the UNHCR's Global Virtual Summit on Digital Identity for Refugees "Envisioning a Digital Identity Ecosystem in Support of the Global Compact on Refugees"' (1 January 2019), UNSW Law Research Paper No. 19–31, https://ssrn.com/abstract=3380116 or http://dx.doi.org/10.2139/ssrn.3380116.

[57] UNHCR, 'From ProGres to PRIMES', Information Sheet 2018 (March 2018), www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-03-16-PRIMES-Flyer.pdf.

[58] Taylor, Simon Michael. "Species ex machina:'the crush'of animal data in AI." BJHS Themes (2023): 1–15.

[59] Fleur Johns, 'Data, detection, and the redistribution of the sensible in international law' (2017) 111(1) *American Journal of International Law* 57–103.

[60] A. Lodinová, 'Application of biometrics as a means of refugee registration: Focusing on UNHCR's strategy' (2016) 2(2) *Development, Environment and Foresight* 91–100.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

advanced modes of biometric data gathering and analysis, some of the current 'international legal thought, doctrine, and practice are, in the main, poorly equipped to deal with them', especially in situations of forced migration.[61] One reason is the lack of manual processing options and how the introduction of machine learning can lift the collection of sensitive and personally identifiable information outside the scope of pre-existing legal methods. In grappling with new forms of quantification and statistics these systems do not just contain hundred-year old statistical decision functions but the pairing of imaging, data aggregation, and machine learning at scale. The autonomy granted to machine learning may remove abilities to interrogate the validity of the earlier datasets and matching results a system relies on to achieve a result. Such logic clusters ever increasing data collections into new 'probabilistic dependencies'.[62] Yet what this curtails are reasonable efforts to disentangle bias from standardised classifications, and how the natural divergences that occur between humans, different social groups, and their situated actions, are erased in deference to the calculative inferences instead. In the use of FRT there is always 'politics attached'. Avi Marciano illustrated this in the context of Israel where biometric standards establish hierarchies for decision making by defining particular bodies as 'ineligible' to access.[63]

Some FRTs are directly complicit in human rights abuses, including a reported detention of up to 1.5 million Uyghur Muslims in Xinjiang.[64] Owing to the increasing scale of an inescapable surveillance that the Chinese Communist Party has funded, ubiquitous CCTV systems and facial recognition are operationalised in public spaces alongside the monitoring of online communications and patterns-of-life data from mobile phones. Idealised as an all-seeing pervasive surveillance network enabled by a state manufacturing of computer vision technology, digital platforms, and data aggregation centres,[65] the simplified idea that Chinese technology and its authoritarian state surveillance system are indigenous is significantly flawed. Before China started using CCTV systems and facial pattern-matching techniques to identify ethnic minorities in Xinjiang Province, Bledsoe proposed to the Defence Department Advanced Research Projects Agency (then known as ARPA)

[61] Ibid., p. 59.

[62] Fleur Johns, 'Global governance through the pairing of list and algorithm' (2016) 34(1) *Environment and Planning D: Society and Space* 126–149.

[63] Marciano, Avi. "The politics of biometric standards: The case of Israel biometric project." Science as Culture 28, no. 1 (2019): 98–119.

[64] In September 2019, four researchers wrote to the publisher Wiley to 'respectfully ask' that it immediately retract a scientific paper. The study, published in 2018, had trained algorithms to distinguish faces of Uyghur people, a predominantly Muslim minority ethnic group in China, from those of Korean and Tibetan ethnicity. C. Wang, Q. Zhang, W. Liu, Y. Liu, and L. Miao, 'Facial feature discovery for ethnicity recognition' (2018) 9(1) *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* Article ID e1278.

[65] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, 'Mapping China's technology giants' (18 April 2019), ASPI Report No. 15, www.aspi.org.au/report/mapping-chinas-tech-giants.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

that it should support Panoramic Research Laboratory in studying the feasibility of using facial characteristics to determine a person's racial background.[66] This is another instance of the politics and the power of FRT recurring and returning and re-playing into new uses, new places, and new eras, yet with similar purposes.

Western companies were involved in the creation of these systems at the start. The export of surveillance technologies from the Global North to China started in the 1970s. It is only now that Chinese technology companies are found competing with and replacing those suppliers in a globalised market.[67] The current status of FRT developed in China with known human rights and privacy violations is not adequately restricted by regulatory frameworks in Europe and the United States.[68] To better disentangle use-cases requires not only a more through mapping of globally entangled and technical supply-chains, whether through critical research or in the building of oversight capabilities such as independent risk assessments, compliance audits, or technical red-teaming in the light of such swiftly evolving material properties.

A contemporary focus on understanding FRT must therefore be concerned not only with the implementation and implications for nation and state-bound privacy law, but to make transparent infrastructural supply chains and situated origins of datasets and technical domains they were created in. This should not simply be restricted to law enforcement and public organisations being required to undertake better procurement strategies – often limited to purchasing orders or responses to requests for information – but to identify the exact sources of the FRT hardware, software, decision functions, and datasets.[69]

Indeed, there are circumstances in which we may need to look further afield. This includes so-called dual-use systems that are adopted not just from domains in nation state and military operations but those trained on animals within precision agriculture.[70] In the shift from classical identification methods to computer vision tools, the future of farming lies in the paddock-to-plate digital identification of each product. Whether for cross-border bio-security purposes or the optimisation of meat

[66] Raviv, 'The secret history of facial recognition'.

[67] Ausma Bernot, 'Transnational state-corporate symbiosis of public security: China's exports of surveillance technologies' (2022) 11(2) *International Journal for Crime, Justice and Social Democracy* 159–173.

[68] Yan Luo and Rui Guo, 'Facial recognition in China: Current status, comparative approach and the road ahead' (2021) 25(2) *University of Pennsylvania, Journal of Law and Social Change* 153.

[69] This includes clarifying information materials to train law enforcement personnel on using and maintaining FRT systems, including manual facial comparison, mobile device uses, and other FRT hardware. Garvie, Bedoya, and Frankle, 'The perpetual line-up'.

[70] See Simon Michael Taylor, 'Species ex machina: 'the crush' of animal data in AI.' (2023) 8 BJHS Themes, 155–169; Ali Shojaeipour, Greg Falzon, Paul Kwan, Nooshin Hadavi, Frances C. Cowley, and David Paul, 'Automated muzzle detection and biometric identification via few-shot deep transfer learning of mixed breed cattle' (2021) 11(1) *Agronomy* 2365, https://doi.org/10.3390/agronomy11112365; and Ali Ismail Awad, 'From classical methods to animal biometrics: A review on cattle identification and tracking' (2016) 123 *Computers and Electronics in Agriculture* 423–435.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

traceability FRT is seen as a viable investment to remotely track animals. These systems commonly utilize open-source software architectures, machine learning and modular camera systems.[71] Yet in the computational transference between animal bodies, digital and data visualisation, and informational materials, we collapse into the heart of Trevor Paglen's art project titled in 'Bloom'. The visualisation and classification of *all images and all bodies* helps to establish the adoption of autonomous methods. This includes initiatives from the global accounting firm KPMG and Meat and Livestock Australia to collect data that translate into efforts to strengthen computer vision market positions. Agribusinesses are not yet treated as handling any sensitive data or training bodily surveillance systems nor are they subjected to regulatory approaches that can throw their data practices into question.[72]

As Mark Maguire suggests, a genealogical and infrastructural approach to FRT 'demands we consider how technologies are an assemblage of different elements delivered from specific contexts' yet re-made, aggregated, customised, adapted, and re-purposed for newly defined, profit-driven, and yet often speculative objectives.[73]

3.5 CONCLUSION

At the time of Bledsoe's experiments there was a meeting between the administrative management of the NYSIIS law enforcement data bases and the computer design company Systems Development Corporation (SDC) of Santa Monica, California, in September 1964.[74] The aim was to decide in what manner to proceed with the implementation of the system, and what techniques to commission for deployment. In summary, the critical inflexion point centred on: 'First buy the computer and decide what

[71] For animal facial recognition biometrics see Yue Lu, Xiaofu He, Ying Wen and Patrick Wang, 'A new cow identification system based on iris analysis and recognition' (2014) 6(1) *International Journal of Biometrics* 18–32.

[72] For regulatory gaps in agricultural data and privacy law, see Annie Guest, 'Are Big Ag Tech companies harvesting farmers' confidential data?' (18 February 2022), *ABC News*, Landline, www.abc.net.au/news/2022-02-19/agriculture-data-protection/100840436; also Kelly Bronson and Phoebe Sengers, 'Big Tech meets Big Ag: Diversifying epistemologies of data and power' (2022) 31(1) *Science as Culture* 1–14; and Leanne Wiseman, Jay Sanderson, Airong Zhang, and Emma Jakku, 'Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming' (2019) 90–91 *NJAS – Wageningen Journal of Life Sciences* 100301.

[73] Mark Maguire, 'The birth of biometric security' (2009) 25 *Anthropology Today* 9–14. This is also because of what has worked in the past – building on successful statistical classifications, image categorisation, and probability.

[74] SDC was called the first software company. It began as a systems engineering group for an air-defence system at the RAND in April 1955 – the same year that 'artificial intelligence' as a term was defined in a Dartmouth Conference proposal. Within a few months, RAND's System Development Division had over 500 employees developing software computing applications. For informational retrieval and database management systems see Jules I. Schwartz, 'Oral history interview with Jules I. Schwartz' (7 April 1989), Center for the History of Information Processing, Charles Babbage Institute. Retrieved from the University of Minnesota Digital Conservancy, https://hdl.handle.net/11299/107628

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

to put on it; (2) Or do an extensive feasibility analysis and, as a result of that study, decide on the computer (how large and powerful) and the functions to be performed.'[75]

As the technical capacity of computing systems in the 1960s was nascent, SDC lacked capability to deliver the required system at scale. Yet this allowed a pause for discussion, consideration, and to recognise that computing capabilities must be defined for a particular purpose, and there should be a thorough vetting of the modular building blocks the system would contain.[76] The title of that report was 'A System in Motion', and it recognised that multiple capabilities – from query and search functions onto image recognition – could not be adequately managed and regulated when developed at once. The NYSIIS report stated the application of computers to solve recognition problems for law enforcement was a foregone conclusion. Yet the question remained whether social institutions and organisations should allow for deploying use of complete automation, especially as they function as a sum of moving, and largely unknown 'experimental parts'?[77]

Although most state departments and law enforcement undertake basic steps to adhere to industry best practices, such as compliance, testing, and legal obligations to avoid public scrutiny, these approaches often lack consistency. FRT is an experimental practice constituted by practices and elements that can be hidden from view, trialed and tested in domains unsuitable to be deemed fit-for-purpose. Whether being trained on exploitative data captured from refugees, prisoners, or operationalised on farm animals, this is called 'the deploy and comply problem' and requires public consultation and impact considerations before being put into action.[78] A prime example is the use of Clearview AI facial algorithms by New Zealand Police in 2020 without consulting the Privacy Commissioner or considering the impacts to vulnerable Indigenous groups.[79] This is indicative of multiple instances of harm,

[75] SDC stressed that it was imperative to get into the computer-design phase as quickly as possible. Their main fear was that if NYSIIS waited too long in getting started, they might not develop a computer system at all. A strong rebuttal was supported by the administrative management of New York State. They felt a Feasibility Report and an exhaustive systems analysis was needed to be completed first. In the end, SDC went along with this decision. See Ross Gallati, 'Identification and intelligence systems for administration of justice', in Cornog et al. (eds.), *EDP Systems in Public Management* (Rand McNally, 1968), pp. 161–162; also Silbert (1970), 'The world's first computerized criminal-justice information-sharing system', p. 116.

[76] Building Block One involved the fingerprint and an ability for the computer to search and summarise case-history capabilities; the second stage was to develop image-recognition on mug shot databases.

[77] B. G. Schumaker, *Computer Dynamics in Public Administration* (Spartan Books, 1967).

[78] Crawford and Calo consider 'this a blindspot in AI' and advocate for analyses at a systems level to consider the history of the data and algorithms being used, and to engage with the social impacts produced at every stage – dataset conception, technology design, use-case deployment and nation-state regulation. Kate Crawford and Ryan Calo, 'There is a blind spot in AI research' (2016) 538 *Nature* 311–313.

[79] New Zealand Police first contacted Clearview in January, and later set up a trial of the software; however, the high tech crime unit handling the technology appears not to have sought the necessary clearance before using it. Mackenzie Smith, 'Police trialled facial recognition tech without clearance' (13

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press

error, oppression, and inequality that have been caused by autonomous decision and surveillance systems.[80] What is needed are efforts to trace, assess, and determine if the modular 'elements' of an FRT system are legitimate, credible, feasible, and reasonable. This challenge seeks to ringfence the 'lineage of intent' – yet can FRT systems be restricted by ethical, legal and technical guardrails to specific, deliberate, and predefined purposes?[81] This is what this book is seeking to address.

May 2020), *Radio New Zealand*, www.rnz.co.nz/news/national/416483/police-trialled-facial-recognition-tech-without-clearance. This resulted in New Zealand Police commissioning a retrospective feasibility and social impacts study owing to the pace of technological change that has outstripped law and regulation. See Nessa Lynch and Andrew Chen, 'Facial recognition technology: Considerations for use in policing' (November 2021), Report commissioned by the New Zealand Police, www.police.govt.nz/sites/default/files/publications/facial-recognition-technology-considerations-for-usepolicing.pdf.

[80] For example, IDEMIA systems have been deployed in different cultural settings with problematic results. IDEMIA supplied the biometric capture kits to the Kenyan government in 2018–2019 for its controversial national digital ID scheme, commonly known as Huduma Namba ('service number'). Data Rights filed a case before the Paris tribunal accusing IDEMIA of failing to adequately address human rights issues. See Frank Hersey, 'NGOs sue IDEMIA for failing to consider human rights risks in Kenyan digital ID' (29 July 2022), BiometricUpdate.com, www.biometricupdate.com/202207/ngos-sue-idemia-for-failing-to-consider-human-rights-risks-in-kenyan-digital-id.

[81] See Manasi Sakpal, 'How to use facial recognition technology ethically and responsibly' (15 December 2021), Gartner Insights, www.gartner.com/smarterwithgartner/how-to-use-facial-recognition-technology-responsibly-and-ethically; and also, Nicholas Davis, Lauren Perry, and Edward Santow, 'Facial recognition technology: Towards a model law' (2022), Human Technology Institute, The University of Technology, Sydney.

https://doi.org/10.1017/9781009321211.005 Published online by Cambridge University Press