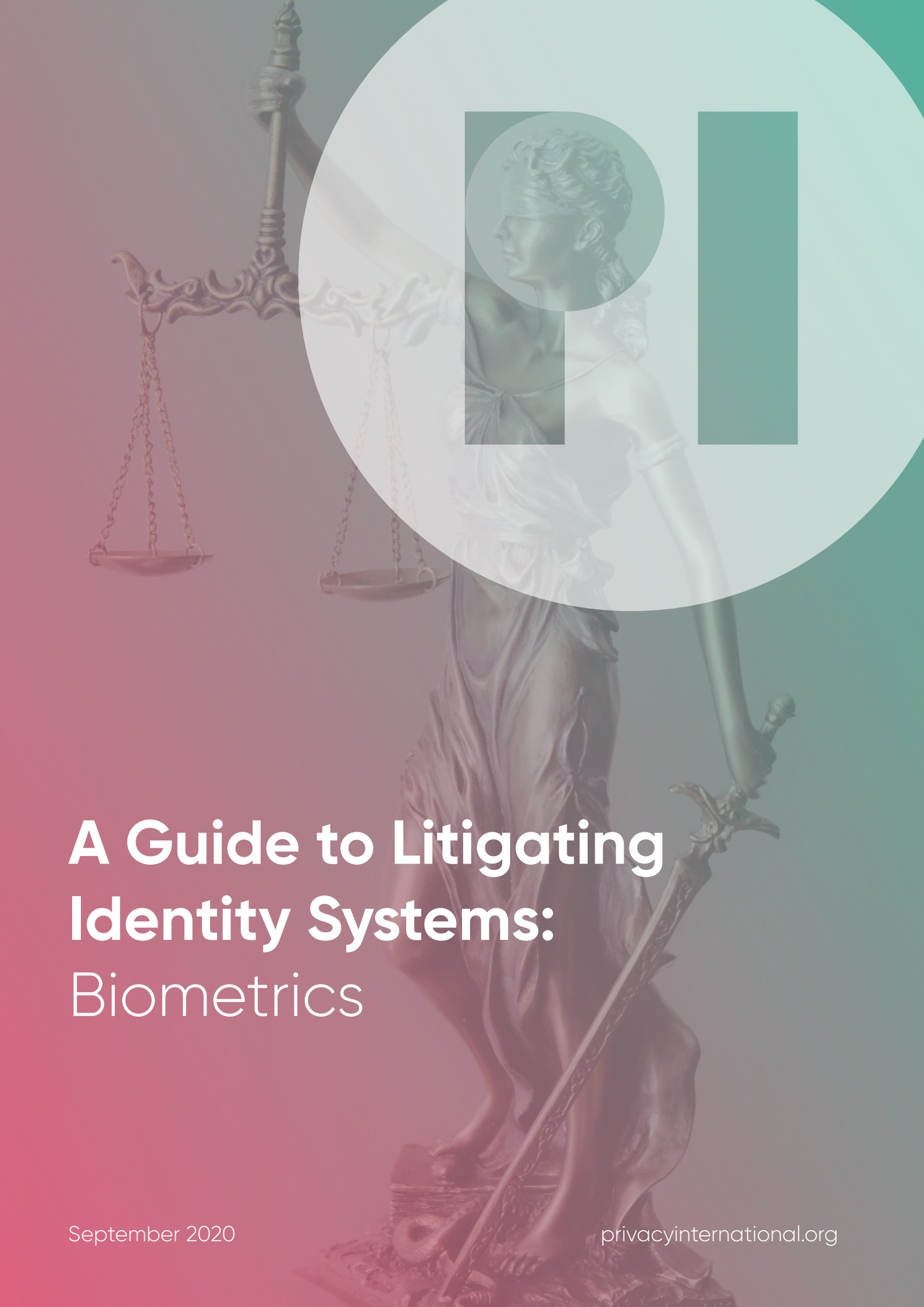

A Guide to Litigating Identity Systems: Biometrics

September 2020

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Privacy International would like to thank Anna Crowe and the International Human Rights Clinic at Harvard Law School for their support in the research, preparation, and drafting of this guide. We are particularly thankful to Clinic students Maithili Pai and Spencer Bateman.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Tingey Injury Law Firm

PART TWO:

BIOMETRICS

WHAT IS BIOMETRIC INFORMATION

46. Biometric information, defined in the Aadhaar legislation as "photograph, finger print, iris scan, or such other biological attributes of an individual as may be specified by regulations,"[160] is often central to the authentication procedures of identity systems. "Authentication" is a process whereby information contained in an identity system (stored locally on a card and/or accessed from a central database) is used to establish whether someone is who they say they are. Identity systems frequently rely on the collection and storage of biometric data during system registration, which is compared with biometric data collected at the point of a given transaction requiring identity system verification.[161] For example, in the Aadhaar system, when an individual seeks to collect a food subsidy, they will be required to provide their Aadhaar number and consent to the collection of their identity information (including biometric data via an iris or fingerprint scan). Their information is sent to the central system authority, which authenticates the identity of the individual by matching the data provided to data stored in the system. The central authority then provides either a positive or negative response to the transmitting vendor. If a positive response is received, the subsidy will be

160 *Aadhaar Judgment*, Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & connected matters, ¶ 40 of dissent (2018).

161 See, eg *Aadhaar Judgment*, ¶ 44 at 51; Madhewoo v. The State of Mauritius and Anor, 2015 SCJ 177 http://ionnews.mu/wp-content/uploads/2015/05/Biometric-ID-Card_Madhewoo-vs-State.pdf at 13; Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 21 (2019).

disbursed.[162] While courts have arguably overstated the effectiveness and necessity of biometric data for identity verification in the past,[163] the frequency of biometric authentication failure[164] is frequently overlooked. These failures can potentially have profoundly negative impacts on individuals enrolled in identity systems,[165] and failures are particularly pronounced in the most vulnerable populations included in identity systems.[166] In addition to the dangers of biometric authentication failure, biometric information uniquely implicates human rights concerns because of its physical nature[167] and the expectation that it will be stored and used over the course of an individual's lifetime.[168]

---

162 See *Aadhaar Judgment*, ¶ 32 at 32–34.

163 See *Aadhaar Judgment*, ¶ 296 at 363.

164 Government of India, Economic Survey 2016–17, **https://www.thehinducentre.com/multimedia/archive/03193/Economic_Survey_20_3193543a.pdf at 194.**

165 See Nikhil Dey & Aruna Roy, "How Chunni Bai's death exposes the lie about Aadhaar," Times of India (30 September 2018), **https://timesofindia.indiatimes.com/home/sunday-times/all-that-matters/how-chunni-bais-death-exposes-the-lie-about-aadhaar/articleshow/66009239.cms**; Privacy International, Understanding Identity Systems Part 3: The Risks of ID, **https://www.privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id**

166 Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis (Springer, 2013), 363.

167 See, eg Madhewoo, 2015 SCJ 177 at 23; *Aadhaar Judgment*, ¶ 127 of dissent; *Opinion of Justice Sykes*, Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 55 (2019).

168 Opinion of Justice Sykes, ¶ 50.

BIOMETRICS AND IDENTITY SYSTEMS

47. This section of the guide provides details on the arguments surrounding biometric information. Advocates and human rights defenders should use these arguments to challenge assumptions about the effectiveness and necessity of biometric data, to explain the unique implications of biometric information on rights, and to frame future arguments developed throughout this guide in identity systems.

Fallibility and inaccuracy

48. The biometric technology underlying identity systems is fallible and not always accurate, leading to authentication failures.

    a) The Jamaican Supreme Court states that because the decision that arises from the biometric matching process is the "outcome of a series of processes that have at their base a probability factor,"[169] it can result in both false positives and false negatives.[170] Additionally, the court states that the differences in sensitivity of the devices executing the initial data collection and subsequent comparison affect the reliability of biometric identity systems and increase the risk of false positives and false negatives.[171] False positives and negatives include instances where the identity of an individually is either incorrectly verified or incorrectly rejected because of the matching of the biometric data.[172]

    b) The dissent of the Indian Supreme Court cites an official document of the Government of India that recorded authentication failures in several

169 *Julian J. Robinson*, ¶ 51.

170 *Julian J. Robinson*, ¶ 51.

171 *Julian J. Robinson*, ¶ 53.

172 See *Opinion of Justice Sykes*, ¶ 51.

states of the country: "While Aadhaar coverage speed has been exemplary, with over a billion Aadhaar cards being distributed, some states report authentication failures: estimates include 49 percent failure rates for Jharkhand, 6 percent for Gujarat, 5 percent for Krishna District in Andhra Pradesh and 37 percent for Rajasthan."[173]

c) The dissent of the Indian Supreme Court cites a report titled "Biometric Recognition: Challenges & Opportunities" by the National Academy of Science USA, which states that biometric recognition systems are inherently probabilistic because biometric characteristics can change as a result of various factors such as "changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, socio-cultural aspects of the situation in which the presentation occurs, changes in human interface with the system, and so on."[174]

d) The Kenyan High Court acknowledges that a "lack of or poor biometric data, such as fingerprints" can lead to failures resulting in exclusion from the national identity system and its attendant services.[175] This finding provided a partial basis for the High Court's determination that a clear regulatory framework must be created in Kenya regulating the manner in which to enrol individuals with "poor biometrics" into the system.[176]

49. Biometric authentication failures have the potential to impact marginalised populations more often.

a) The dissent of the Indian Supreme Court in the *Aadhaar* judgment cites excerpts from academic scholarship on the topic, including books that state the error rates in biometric systems are particularly high for the young, the aged, disabled persons, as well as persons suffering from

173 Government of India, Economic Survey 2016–17 at 194.

174 Joseph N. Pato and Lynette I. Millett, eds., Biometric Recognition: Challenges & Opportunities (National Academy of Science USA, 2010), https://www.nap.edu/read/12720/chapter/1

175 *Huduma Namba Judgment*, Nubian Rights Forum and Others v. The Hon. Attorney General, Consolidated Petitions No. 56, 58 & 59 of 2019 ¶ 1012 (2020).

176 *Huduma Namba Judgment*, ¶ 1012 (2020).

health problems.[177] The dissent also cites a government report that suggests manual labourers will be disparately affected by biometric failures because their fingerprints change as a result of the rough nature of their work.[178]

b) The Kenyan High Court specifies: "there may be a segment of the population who run the risk of exclusion" due to biometric failures, as well as other identity system registration failures.[179] Although the court does not indicate a segment or segments of the population, expert testimony referenced in the court's summary of the record earlier in the judgment states that biometric parameters may change over the course of an individual's life.[180]

Not the only tool for identification and authentication

50. The biometric technology underlying identity systems is not the only way to authenticate an individual's identity.

a) Justice Sykes opinion in the Jamaican case finds that the government has not shown a compelling need to subject Jamaicans to a compulsory biometric data collection,[181] and the government failed to show that only necessary information was being collected.[182] While the opinion does not specify what alternative authentication methods exist, the court's scepticism that the government proved the programme's data minimisation suggests an assumption that a less invasive method is available.

177 *Kindt*, Privacy and Data Protection Issues, 363.

178 *Aadhaar Judgment*, ¶ 111 of dissent.

179 *Huduma Namba Judgment*, ¶ 1012.

180 *Huduma Namba Judgment*, ¶ 36.

181 *Opinion of Justice Sykes*, ¶ 247(B)(52).

182 *Opinion of Justice Sykes*, ¶ 247(B)(57).

b) The Judicial Yuan in Taiwan argued that compulsory fingerprinting was unnecessary for the identity card system the government sought to introduce in Taiwan.[183] In particular, the Judicial Yuan identified existing anti-fraud components, other than fingerprints, of identity cards that are designed to prevent fraud.[184]

Intrusive nature

51. The use of biometric data in identity systems is uniquely problematic because of the data's physical nature. The data's unique status as a part of a person's body, as in the case of fingerprints and iris scans, raises concerns of sensitivity and control of one's own body.

    a) The Mauritian court relies on the physical nature of fingerprint data in finding how the country's limited search-specific right to privacy was implicated.[185] The fingerprinting requirement was evaluated as a physical search of the person, which allowed the court to examine the constitutionality of the fingerprinting requirement even where there was not a generally protected right to privacy in that country.[186] In Mauritius, the constitutional right to be free from unlawful search and seizure requires that a search only be permitted in the interests of public order, except when that search is shown to be reasonably unjustifiable in a democratic society.[187]

    b) The dissenting opinion in the *Aadhaar* judgment notes the threat to bodily privacy posed by biometric data.[188] The dissent notes that the collection

183 Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005).

184 Judicial Yuan Interpretation No. 603, Taiwan, Holding (2005).

185 *Madhewoo*, 2015 SCJ 177 at 23.

186 *Madhewoo*, 2015 SCJ 177 at 23.

187 *Madhewoo*, 2015 SCJ 177 at 24.

188 *Aadhaar Judgment*, ¶ 125–26 of dissent.

of biometric data results in a physical intrusion, which can cause mental harm for people of specific cultural or religious backgrounds.[189]

c) Justice Sykes of the Jamaican Supreme Court points out that biometric data can reveal personal information about an individual's physical health.[190] For example, Justice Sykes suggests biometric data like retina and iris scans, as well as fingerprints, can be used to determine if an individual has Down's syndrome, hypertension, or diabetes.[191] Health data is particularly sensitive because it may reveal an individual's medical conditions, which can have "devastating privacy consequences for the individual."[192]

d) The Kenyan High Court finds biometric data collected by the Kenyan national identity system to be "personal, sensitive, and intrusive data that requires protection."[193] In reaching this conclusion, the court references the biometric data's ability to be collected without an individual's knowledge or consent,[194] with potential serious social, reputational, or legal risks and consequences resulting from biometric data's unauthorised disclosure,[195] and the ability of biometric data to provide personal information about an individual.[196] Moreover, the court also argues that one particular form of biometric data – DNA information – can reveal an individual's "likeliness to develop particular diseases, parentage and also family links."[197]

---

189 *Aadhaar Judgment*, ¶ 127 of dissent.

190 Opinion of Justice Sykes, ¶ 55.

191 Opinion of Justice Sykes, ¶ 55.

192 Opinion of Justice Sykes, ¶ 55.

193 *Huduma Namba Judgment*, ¶ 772.

194 *Huduma Namba Judgment*, ¶ 767.

195 *Huduma Namba Judgment*, ¶ 762.

196 *Huduma Namba Judgment*, ¶ 758.

197 *Huduma Namba Judgment*, ¶ 916.

Permanence

52. The use of biometric data in identity systems is similarly problematic because it is stored indefinitely for the duration of a person's life and potentially beyond. This highlights the importance of storage limitation, which serves as a safeguard by limiting the duration for which data is processed and stored.

    a) While related partly to the digital nature of data storages and breaches, Jamaican Supreme Court Justice Sykes suggests that once a biometric system breach has occurred, it cannot be reversed.[198] As a result, an individual's biometric data will be exposed forever.

    b) The Kenyan High Court argues that the misuse of biometric data is dangerous because biometrics are "uniquely linked with individuals," "cannot be changed and are universal," and because "the effects of any abuse of [sic] misuse of the data are irreversible."[199] The irreversibility of misuse of biometric data is amplified when the data is centrally stored because data subjects will most often lack information or control over the use of data stored in that manner.[200]

    c) The majority opinion in the *Aadhaar* judgment does not make the connection between biometrics and permanence expressly. However, the court restricts the time for which data can be stored partly on the grounds that the right to be forgotten would be infringed by lengthy storage of data.[201] The court limits the time for which authentication transaction data can be stored from five years to six months.[202]

198 *Opinion of Justice Sykes*, ¶ 50.

199 *Huduma Namba Judgment*, ¶ 880.

200 *Huduma Namba Judgment*, ¶ 880.

201 *Aadhaar Judgment*, ¶ 205 at 282.

202 *Aadhaar Judgment*, ¶ 205 at 282.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org