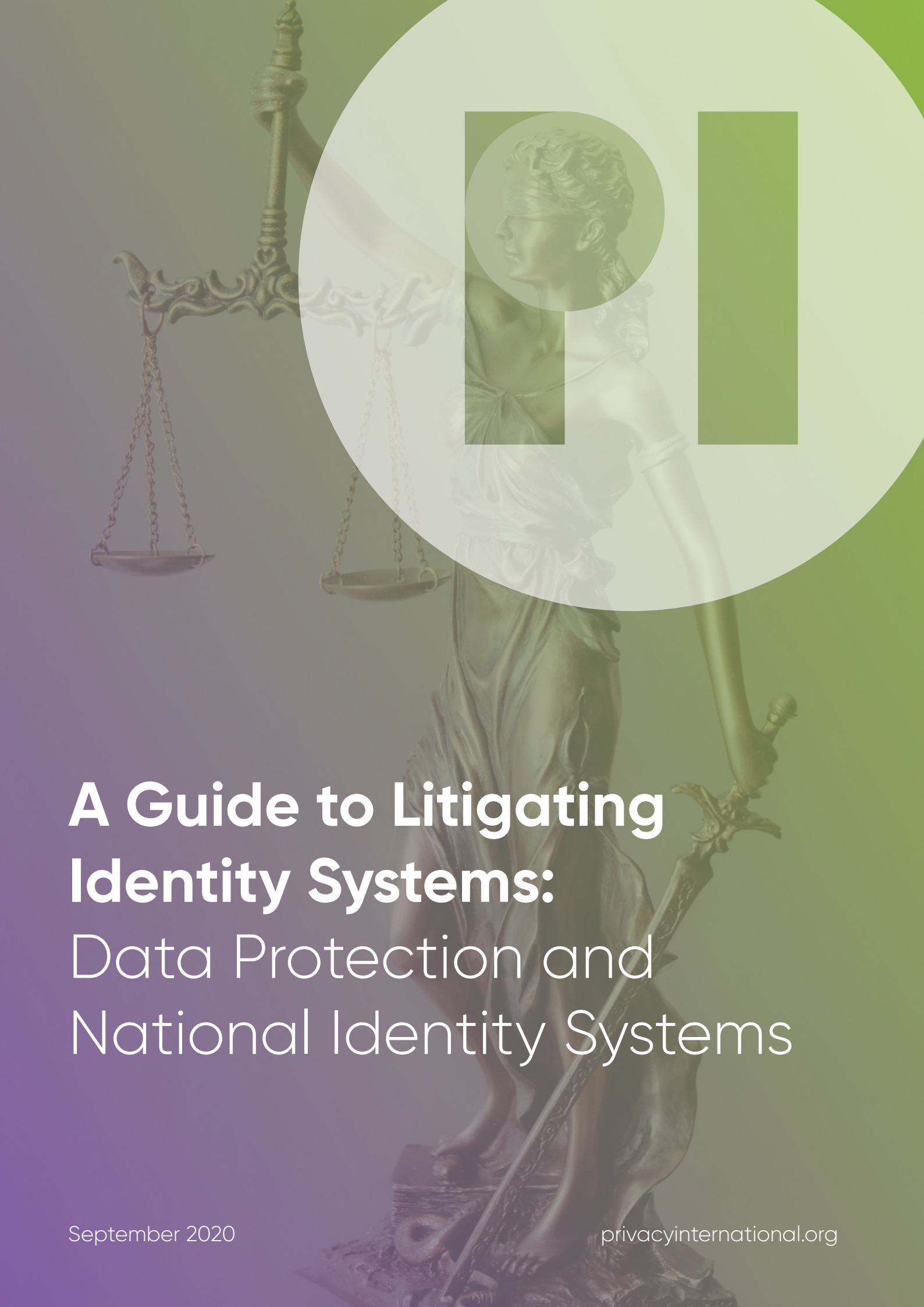

A Guide to Litigating Identity Systems: Data Protection and National Identity Systems

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 THREE:

DATA PROTECTION AND NATIONAL IDENTITY SYSTEMS

53. National Identity Systems naturally implicate data protection issues, given the high volume of data necessary for the systems' functioning. Identity systems collect and store biometric and demographic data obtained at the time of enrolment in the systems,[203] as well as transaction data obtained when the system is used to verify an individual's identity.[204] This wide range and high volume of data implicates issues of consent, as individuals should be aware and approve of their data's collection, storage, and use if the system is to function lawfully.[205] Despite this, identity systems often lack necessary safeguards requiring consent[206] and the mandatory nature of systems ignores consent entirely.[207] Additionally, identity systems have a propensity to extend in application beyond their initial conception into numerous areas of public and private life,[208] spreading individuals' data to numerous actors without their consent and consideration. Even where the

203 See *Aadhaar Judgment*, Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & connected matters ¶ 446 at 524.

204 See *Aadhaar Judgment*, ¶ 197 at 276 (2018).

205 See *Aadhaar Judgment*, ¶ 304 of dissent.

206 See *Aadhaar Judgment*, ¶ 304 of dissent.

207 See *Opinion of Justice Batts*, *Julian J. Robinson* v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 349 (2019).

208 *Opinion of Justice Sykes*, *Julian J. Robinson* v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 247(B)(56) (2019).

54. system is legislatively prescribed to be voluntary, the spread of requirements across public and private life make consent arguably illusory. The most vulnerable populations are at greater risk of losing the practical ability to withhold consent because of the power imbalances that exist between individuals and the state. This issue is further complicated by widespread sharing of data among public and private actors involved in the identity system's administration and application.[209] This sharing occurs without safeguards and judicial oversight in many contexts.[210] Finally, multinationals are frequently involved in the design and implementation of identity systems, further expanding the scope of data sharing involved in the systems.[211] Without these safeguards, there can be no guarantee that an identity system is implicating privacy rights in the least intrusive way to accomplish state objectives.[212]

55. This section of the guide illustrates arguments surrounding data protection law and its relationship to identity systems, while providing context from several of the national court judgments analysing the systems. Advocates and human rights defenders should use these arguments to challenge the implementation of identity systems designed without the requisite internal safeguards and background data protection frameworks to protect individuals' rights.

209 See *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 32.

210 *Aadhaar Judgment*, ¶ 339(14)(f) of dissent.

211 See *Aadhaar Judgment*, ¶ 232 of dissent.

212 *Aadhaar Judgment*, ¶ 306 of dissent.

CONSENT IN DATA COLLECTION AND USE

56. Without robust data protection requirements that include an individual's consent to their data's collection and use, a national identity system fails to adequately protect subjects of the system.

    a) The absence of consent renders the Aadhaar system unconstitutional in the eyes of the dissenting opinion from the Indian Supreme Court. With respect to the Section 59 savings provision of the system's enacting legislation, which would have retroactively validated the actions of the Central Government taken before the Aadhaar legislation was passed, the dissent finds that the failure to obtain informed consent and the lack of procedural safeguards in the system between 2009 and 2016 make that provision unconstitutional.[213] Section 29(4) of the legislation, which prohibited the publishing of data collected under the scheme except where allowed under the governing regulations, is also found unconstitutional by the dissenting opinion because of inadequate informed consent in the collection of biometric data under the regulations specifying when an individual's data may be published, displayed, or posted.[214] More generally, the dissent finds that the absence of a comprehensive data protection framework leaves the identity system vulnerable to serious violations of privacy.[215] The existing data protection laws at the time acknowledged the importance of consent, but failed to adequately address the breadth of the system and its privacy right implications.[216]

    b) The issue of consent underwrites much of the Jamaican Supreme Court's analysis of the constitutionality of a proposed Jamaican national identity

213 *Aadhaar Judgment*, ¶ 304 of dissent.

214 *Aadhaar Judgment*, ¶ 339(9) of dissent.

215 *Aadhaar Judgment*, ¶ 306 of dissent.

216 See *Aadhaar Judgment*, ¶ 306 of dissent.

system. Justice Sykes, while discussing the right to privacy in Jamaica generally, focuses much of his analysis on the concept of choice.[217] In finding the system unconstitutional, Justice Sykes cites the improper compulsory taking of biometric information from individuals.[218] Justice Batts echoes this view, finding that the right to privacy is violated partly because of the absence of a right to opt out of the system.[219] Justice Batts also finds the provision of the system requiring the establishment of a national database for the "collection and collation of identity information and demographic information regarding registrable individuals" constitutional, where the data included in the database is voluntarily given, although the system as a whole is rejected.[220] Each of these facets of the Jamaican Supreme Court's analysis points to the particular importance of consent in the constitutionality of an identity system.

c) The Mauritian Supreme Court highlights the absence of sufficient safeguards for the use of fingerprint data stored as part of the Mauritian national identity system.[221] In particular, the court isolates the provisions of the Mauritian Data Protection Act, which create exceptions to the requirement that an individual's express consent is obtained prior to the processing of personal biometric data.[222] The relevant data protection regime would allow for the sharing of data without consent to many actors, including law enforcement, artists, healthcare providers, financial firms, and lawyers.[223] The absence of individual consent for such access, in

217 See Opinion of Justice Sykes, ¶ 247(A)(10).

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

219 Opinion of Justice Batts, ¶ 349.

220 Opinion of Justice Batts, ¶ 348.

221 *Madhewoo*, 2015 SCJ 177 at 29–34.

222 *Madhewoo*, 2015 SCJ 177 at 32.

223 *Madhewoo*, 2015 SCJ 177 at 32.

conjunction with the absence of judicial oversight of the regime, defeated the storage of fingerprint data's constitutionality.[224]

d) The majority opinion in the *Aadhaar* judgment centres its discussion of the possible deficiencies of consent in the collection of identity system data around children. The majority determines that because children cannot provide legal consent, their participation in the system relies on their parents' consent.[225] Once a child reaches the age of majority – when they can provide legal consent – they must be given the option to exit the system.[226]

e) The Kenyan High Court cites the necessity of both knowledge and consent of data subjects as an international principle underlying data protection requirements.[227] Although the court broadly finds that consent is sufficiently contemplated by the Kenyan national identity system, the ability to obtain and use DNA information and GPS coordinates without knowledge or consent is a primary reason for the court's ruling that neither the collection nor use of those types of data is permissible.[228]

224 *Madhewoo*, 2015 SCJ 177 at 32–34.

225 *Aadhaar Judgment*, ¶ 332 at 401.

226 *Aadhaar Judgment*, ¶ 332 at 401.

227 *Huduma Namba Judgment*, Nubian Rights Forum and Others v. The Hon. Attorney General, Consolidated Petitions No. 56, 58 & 59 of 2019 ¶ 844 (2020) (referencing the OECD Privacy Principles).

228 See Huduma Namba Judgment, ¶ 767.

FUNCTION CREEP AND IDENTITY SYSTEMS

57. The collection and storage of data necessary for a national identity system creates a risk of function creep, which is the proliferation of the identity system's uses for public and private programmes and purposes.

    a) The majority opinion from the Indian Supreme Court in the *Aadhaar* judgment identifies and limits numerous examples of potential function creep. The majority finds the requirement of linking with Aadhaar unconstitutional with respect to education,[229] banking,[230] and mobile phone use.[231]

        a) With respect to education, the court finds that requiring Aadhaar for admission extends beyond the permissible scope of the enacting legislation, as compulsory education is not a service, subsidy, or benefit.[232]

        b) In relation to banking, the majority finds that the linking of Aadhaar to banking for the purpose of combatting money laundering fails the proportionality test employed with respect to the right to privacy because the interferences with privacy and property outweighed any potential benefits in preventing money laundering.[233]

        c) With respect to mobile phone use, the majority finds that the requirement of linking Aadhaar with SIM cards is too intrusive to justify under the proportionality framework.[234]

---

229 *Aadhaar Judgment*, ¶ 332 at 401–402.

230 *Aadhaar Judgment*, ¶ 447 at 556.

231 *Aadhaar Judgment*, ¶ 442 at 521.

232 *Aadhaar Judgment*, ¶ 332 at 401.

233 *Aadhaar Judgment*, ¶ 447 at 556.

234 *Aadhaar Judgment*, ¶ 442 at 521.

A unique function creep concern is implicated in these instances either because the application of the identity system extends beyond its statutory basis or the domain in which the system is extended meaningfully changes the applicable balancing under proportionality.

b) The dissenting opinion in the *Aadhaar* judgment also identifies these instances of function creep. Additionally, the dissent notes a general concern of potential function creep by identifying the enacting legislation's breadth and ambiguous language as giving rise to function creep.[235] The dissent then points out that the Aadhaar system has been extended to 252 government schemes, ranging from children's essay contest submissions to the receipt of food subsidies. The list of schemes the dissent provides illustrates the breadth of Aadhaar's reach into everyday life:

> *"[Schemes Aadhaar is required to include] schemes for children (such as benefits under the Sarva Shiksha Abhiyan or getting meals under the Mid-day meal scheme, painting and essay competitions for children, scholarships on merit), schemes relating to rehabilitation of bonded labour and human trafficking, scholarship schemes for SC/ST [Scheduled Caste (SCs) and Scheduled Tribes (STs)] students, universal access to tuberculosis care, pensions, schemes relating to labour and employment, skill development, personnel and training, agriculture and farmers' welfare, primary and higher education, social justice, benefits for persons with disabilities, women and child development, rural development, food distribution, healthcare, Panchayati Raj, chemicals and fertilizers, water resources, petroleum and natural gas, science and technology, sanitation, textiles, urban development, minority affairs, road transport, culture, tourism, urban housing, tribal affairs and stipends for internship for students."*[236]

235 *Aadhaar Judgment*, ¶ 246 of dissent.

236 *Aadhaar Judgment*, ¶ 246 of dissent.

c) Justice Sykes of the Jamaican Supreme Court briefly mentions function creep, stating that the risk of function creep, which would further jeopardise privacy rights, is greater where data minimisation principles are not followed.[237]

d) The Kenyan High Court also briefly mentions function creep, indicating the court is "persuaded" by expert testimony that included an argument that "the mere existence of data in a centralised identification system leads to the temptation to use it for purposes not initially intended."[238] The court's acceptance of the broader testimony, including this statement, contributed to its conclusion that the data protection framework governing the Kenyan national identity system was inadequate.[239]

237 *Opinion of Justice Sykes*, ¶ 247(B)(56).

238 *Huduma Namba Judgment*, ¶ 877.

239 *Huduma Namba Judgment*, ¶ 885.

DATA SHARING

58. The absence of a data protection framework limiting the extent to which private and public actors can access identity system data makes an identity system incompatible with privacy rights and democratic values.
    a) The Mauritian Supreme Court finds that the indefinite storage of fingerprint data used by the Mauritian national identity system was impermissible because of the ease of access to fingerprint data by a wide range of actors with little judicial oversight.[240] Actors capable of accessing the data under the Mauritian Data Protection Act included law enforcement, artists, healthcare providers, financial firms, and lawyers.[241] While the court identifies the storage of fingerprint data as satisfying the initial requirements of a public order exception to the Mauritian Constitution's protection against searches,[242] the storage practice does not satisfy the limitation of the exception requiring the practice be "reasonably justifiable in a democratic society."[243]
    b) The Jamaican Supreme Court also takes issue with data-sharing provisions included within the national identity system in Jamaica, which at the time of the decision did not have a complementary standalone data protection law.[244] Justice Sykes finds that provisions of the identity system legislation that allowed for third-party access to the system database were unconstitutional because of a lack of safeguards.[245] Justice Sykes suggests that data must be relevant and not excessive in relation to the purpose for which it is stored and data must not be stored

240 *Madhewoo*, 2015 SCJ 177 at 32–33.

241 *Madhewoo*, 2015 SCJ 177 at 32.

242 *Madhewoo*, 2015 SCJ 177 at 29.

243 *Madhewoo*, 2015 SCJ 177 at 34.

244 *Opinion of Justice Sykes*, ¶ 3.

245 *Opinion of Justice Sykes*, ¶ 247(B)(115).

for longer than is necessary.[246] Additionally, Justice Sykes rejects third-party access to the system's data because of a lack of incentives for third parties to protect and safely discard data.[247]

c) The majority in the *Aadhaar* judgment restricted the extent to which provisions of the system's enacting legislation allowed for private party access to the Aadhaar database. Section 57 of the law would have allowed "any body corporate or pursuant" to request Aadhaar identity verification "for any purpose."[248] The majority finds the provision does not "pass the muster of proportionality doctrine" while paying particular attention to the weakness of the public interest component of proportionality balancing with regard to private authentication.[249] The majority further limits data sharing in relation to public actors in the national security context. The majority restricts data sharing with national security services by raising the requisite rank of the officer determining the need for disclosure and requiring judicial involvement in the disclosure process.[250]

d) The dissenting opinion in the *Aadhaar* judgment also restricts Section 57 of the system's enacting legislation, finding that private actor access to the Aadhaar platform extends beyond the purpose of the legislation for ensuring targeted delivery of social welfare benefits.[251]

59. National Identity Systems impermissibly infringe upon individual rights when the data protection regimes governing the system's sharing of data with security services fail to include robust safeguards.

a) Members of the Jamaican Supreme Court express particular concern with the proposed Jamaican identity system's data sharing with state security services. Justice Palmer Hamilton finds there are insufficient safeguards in

246 *Opinion of Justice Sykes*, ¶ 247(B)(67).

247 *Opinion of Justice Sykes*, ¶ 247(B)(74–76).

248 *Aadhaar Judgment*, ¶ 355 at 427–428.

249 *Aadhaar Judgment*, ¶ 363–66 at 432–434.

250 *Aadhaar Judgment*, ¶ 447 at 559.

251 *Aadhaar Judgment*, ¶ 243 of dissent.

the system to prevent data profiling.[252] Justice Batts similarly determines that the system lacks requisite safeguards appropriately balancing the benefits of disclosure for security purposes with the right to privacy.[253] Inadequate safeguards that Justice Batts identifies include no opportunity for a hearing,[254] broad wording of conditions under which data sharing is allowed,[255] and no law regulating the time period for which data will be retained.[256] Justice Sykes also states that heightened safeguards are necessary when data can be used for police purposes.[257]

b) The majority opinion in the *Aadhaar* judgment restricts the extent to which data can be shared for the purpose of protecting national security. The majority seeks to accomplish this restriction by requiring that the determination for when data is to be shared is made by an officer of a higher rank than included in the enacting legislation's provisions.[258] Additionally, the majority requires a judicial officer's involvement in the process for determining when data can be disclosed for this purpose.[259]

60. Government authorities must be transparent about the scope and use of their data processing activities. An important element of the rule of law is judicial oversight – an element that takes on particular significance in the implementation of identity systems given their wide-ranging implications on individuals rights and liberties. Judicial oversight is necessary if data collected or stored pursuant a national identity system is to be shared.

---

252 *Opinion of Justice Palmer* Hamilton, *Julian J. Robinson* v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 375 (2019).

253 *Opinion of Justice Batts*, ¶ 365–66.

254 Opinion of Justice Batts, ¶ 366.

255 *Opinion of Justice Batts*, ¶ 365.

256 *Opinion of Justice Batts*, ¶ 366.

257 *Opinion of Justice Sykes*, ¶ 247(B)(67).

258 *Aadhaar Judgment*, ¶ 447 at 559.

259 *Aadhaar Judgment*, ¶ 447 at 559.

a) The Mauritian Supreme Court identifies the lack of judicial oversight over the data-sharing regime in which the Mauritian identity system would operate as particularly problematic, citing it as a reason for the court's decision to hold the storage regime to be unconstitutional.[260]

b) Justice Batts of the Jamaican Supreme Court finds that the lack of a hearing procedure to be used when Jamaican identity system data is disclosed to security services renders the provision unconstitutional.[261]

c) The majority opinion in the *Aadhaar* judgment applies a judicial process safeguard in its determination that the national security data-sharing provisions of the Aadhaar system are unconstitutional.[262] Additionally, the majority finds that Section 47 of the Aadhaar system's enacting legislation (which allowed only the government to lodge a complaint alleging a violation of the system legislation in court) should be amended to allow for an individual's right to file a claim and initiate proceedings when their rights are violated.[263]

d) The dissenting opinion in the *Aadhaar* judgment similarly finds Section 47 of the system's enacting legislation unconstitutional because it "fails to provide a mechanism to individuals to seek efficacious remedies for violation of their right to privacy."[264]

260 *Madhewoo*, 2015 SCJ 177 at 32–33.

261 Opinion of Justice Batts, ¶ 366.

262 *Aadhaar Judgment*, ¶ 447 at 559.

263 *Aadhaar Judgment*, ¶ 353 at 427.

264 *Aadhaar Judgment*, ¶ 339(14)(f) of dissent.

MULTINATIONAL INVOLVEMENT IN IDENTITY SYSTEMS

61. The involvement of multinationals in the implementation of national identity systems heightens the risk of privacy violations caused by improper access to personal data.

    a) The dissenting opinion in the *Aadhaar* judgment notes the system's contract with L-1 Identity Solutions, an American company, through which the biometric software used by the system is licensed from the company.[265] The dissent notes that the contract's terms could allow for access to personal information by the company without an individual's consent.[266]

265 *Aadhaar Judgment*, ¶ 231 of dissent.

266 *Aadhaar Judgment*, ¶ 232 of dissent.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org