



A Guide to Litigating Identity Systems: Impact on Rights other than Privacy

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.



Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

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 FOUR:

IMPACT ON RIGHTS OTHER THAN PRIVACY

62. While identity systems pose grave dangers to the right to privacy, based on the particularities of the design and implementation of the identity system, they can also impact upon further fundamental rights and freedoms upheld by other international human rights instruments, including the International Covenant on Civil and Political Right and the International Covenant on Economic, Social and Cultural Rights such as the right to be free from unlawful discrimination, the right to liberty, the right to dignity, and the right to equality. The risks of exclusion – which implicates a variety of rights ranging from civil and political rights, such as the right to stand for and hold office, as well as socio-economic rights such as the right to food and the right to education – are exacerbated in biometric identity systems due to authentication failures, with heightened impacts on marginalised and vulnerable groups, particularly in developing countries with weak legal frameworks. Systems that are created with a goal of providing legal identity and furthering social, economic, and financial inclusion become the basis for exclusion from access to goods and services and denial of fundamental human rights, leading to complete disenfranchisement of the individual. Thus, it is crucial that the decision to adopt an identity system is informed by the grave concerns that have been highlighted in the judgments on identity systems.

THE RIGHT TO LIVE IN DIGNITY

63. Identity systems violate the dignity of individuals.

- a) The dissent of the Indian Supreme Court in the *Aadhaar* judgement holds that the arbitrary exclusion of individuals from benefits and subsidies to which they are entitled is a violation of dignity.²⁶⁷
- b) The dissent of the Indian Supreme Court in the *Aadhaar* judgement holds that because social security schemes were introduced to protect the dignity of the marginalised, exclusion from these schemes as a result of Aadhaar violates the dignity of the individual.²⁶⁸
- c) The dissent of the Indian Supreme Court in the *Aadhaar* judgement holds that while efficiency is a significant facet of institutional governance, it cannot be a justification to compromise dignity.²⁶⁹
- d) The Jamaican Supreme Court holds that the right to privacy recognises that a person's biometric information is theirs and that they retain control over that information by virtue of their inherent dignity as free autonomous beings.²⁷⁰
- e) The Jamaican Supreme Court holds that the inherent dignity of all human beings includes the right of the individual "to be left alone, the right to be anonymous and to retain control over their home, body, mind, heart and soul."²⁷¹

267 *Aadhaar Judgment*, Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & connected matters, ¶ 262 of dissent (2018).

268 *Aadhaar Judgment*, ¶ 253 of dissent.

269 *Aadhaar Judgment*, ¶ 13 of dissent.

270 *Julian J. Robinson v. The Attorney General of Jamaica*, Claim No. 2018HCV01788, ¶247(B)(10) (2019).

271 *Julian J. Robinson*, ¶ 247(B)(11).

RIGHTS TO LIBERTY AND MOVEMENT

64. Identity systems impact the right to liberty.

- a) The Jamaican Supreme Court holds that the right to liberty includes the right to choose whether or not to share personal information and that the requirement under the identity system's legislation to compulsorily part with biographical and biometric information without having the right to opt out is likely to violate Article 13(3)(a) of the Jamaican Charter of Fundamental Rights and Freedoms, which protects "the right to life, liberty and security of the person and the right not to be deprived thereof except in the execution of the sentence of a court in respect of a criminal offence of which the person has been convicted."²⁷²
- b) The Jamaican Supreme Court held that the right to physical liberty is affected due to the freedom of movement being constrained by requiring an individual to go to a specific place at a specific time to give the information mandated under the legislation.²⁷³
- c) The dissent of the Indian Supreme Court holds that liberty involves not only a negative component but also a positive component that requires states to take positive measures to protect individual rights by creating a data protection regime and autonomous regulatory frameworks that give individuals access to remedies against both state and non-state actors.²⁷⁴

²⁷² *Julian J. Robinson*, ¶ 349.

²⁷³ *Julian J. Robinson*, ¶ 247(B)(19), 361.

²⁷⁴ *Aadhaar Judgment*, ¶ 169 of dissent.

RIGHT TO EQUALITY AND NON-DISCRIMINATION: EXCLUSION

65. Identity systems can lead to discrimination between different groups of persons, particularly in the absence of a strong legal framework.

- a) The Supreme Court of Jamaica found that that country's proposed identity system violated the right to equality, guaranteed under Jamaica's Constitution, because it treated Jamaican citizens less favourably than foreigners. The legislation creating the system would have required Jamaican citizens and "ordinary" residents of Jamaica to produce the National Identity Number or National Identity Card when they sought to gain access to goods and services provided by public bodies. However, foreigners would have had the option to provide other means of identification for access to services.
- b) The dissent of the Indian Supreme Court points to numerous instances in history where the "persecution on the basis of race, ethnicity and religion was facilitated through the use of identification systems,"²⁷⁵ and emphasises the need to take into account lessons learnt from history to carefully monitor the development of identification systems.²⁷⁶
- c) The dissent of the Indian Supreme Court cites Privacy International's report on biometrics²⁷⁷, which states that in the absence of strong legal frameworks and strict safeguards, the application of biometric technologies can be broadened to facilitate discrimination.²⁷⁸

275 Aadhaar Judgment, ¶ 128 of dissent.

276 Aadhaar Judgment, ¶ 128 of dissent.

277 Privacy International, Biometrics: friend or foe of privacy?, December 2013.
<https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy>

278 Aadhaar Judgment, ¶ 120 of dissent.

66. As discussed in an earlier chapter, 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,”²⁷⁹ it can result in both false positives and false negatives.²⁸⁰
 - b) The Jamaican Supreme 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.²⁸¹
 - c) The dissent of the Indian Supreme Court cites an official document of the Government of India which recorded authentication failures in several 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.”²⁸²

279 Julian J. Robinson, ¶ 51.

280 Julian J. Robinson, ¶ 51.

281 Julian J. Robinson, ¶ 53.

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

- d) 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."²⁸³
67. Identity systems disproportionately impact the rights of marginalised and vulnerable people, compounding and multiplying factors of exclusion.
- a) The dissent of the Indian Supreme Court observes that while Aadhaar is likely to cover every basic aspect of the lives of all citizens, the impact is particularly adverse for marginalised citizens who are dependent on the government's social security schemes and other welfare programmes for survival.²⁸⁴
- b) The dissent of the Indian Supreme Court cites a household survey that found the the effect of exclusion was particularly heightened for vulnerable populations like widows, the elderly, and manual workers.²⁸⁵
- c) The dissent of the Indian Supreme Court cites a report of pension being denied to individuals suffering from leprosy, as the condition can damage fingerprints, creating barriers in biometric enrolment.²⁸⁶

283 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>

284 *Aadhaar Judgment*, ¶ 246 of dissent (2018).

285 Jean Drèze, Nazar Khalid, Reetika Khera, and Anmol Somanchi, "Aadhaar and food security in Jharkhand: Pain without gain?," *Economic & Political Weekly*, vol. 52 (16 December 2017).

286 Puja Awasthi, "Good enough to vote, not enough for Aadhaar," *People's Archive for Rural India*, <https://ruralindiaonline.org/articles/good-enough-to-vote-not-enough-for-aadhaar/>

- d) The dissent of the Indian Supreme Court 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 health problems.²⁸⁷
- e) The Kenyan High Court notes that “there may be a segment of the population who run the risk of exclusion” in particular.²⁸⁸ This statement follows the court’s earlier discussions of the potential changing of biometrics over time,²⁸⁹ as well as difficulties of pastoral communities in obtaining documentation necessary for enrolment.²⁹⁰

68. Identity systems can lead to the perpetuation of pre-existing inequalities and injustices.

- a) The dissent of the Indian Supreme Court warns that the quest for technology cannot be oblivious to the “real problems” in India²⁹¹ and that the digital divide in India can lead to the perpetuation of pre-existing inequalities: *“Large swathes of the population have little or no access to the Internet or to the resources required for access to information... While data is the new oil, it still eludes the life of the average citizen. If access to welfare entitlements is tagged to unique data sets, skewed access to informational resources should not lead to perpetuating the pre-existing inequalities of access to public resources.”*²⁹² The dissent also cites the opinion of Jean Drèze that the biometric technology underlying identity systems is inappropriate for rural India and a “recipe for chaos,” especially

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

288 *Huduma Namba Judgment*, ¶ 1012.

289 See *Huduma Namba Judgment*, ¶ 36.

290 See *Huduma Namba Judgment*, ¶ 1006.

291 *Aadhaar Judgment*, ¶ 269 of dissent.

292 *Aadhaar Judgment*, ¶ 10 of dissent.

in villages with poor connectivity where technological glitches immobilise the system.²⁹³

- b) The dissent of the Indian Supreme Court also cites excerpts from a book that states the systems intended to provide assistance and help people out of poverty can become systems of perpetuating poverty and injustice due to problems in authentication and algorithmic technology.²⁹⁴
- c) The Kenyan High Court notes that enrolment may be more difficult for members of pastoral communities that lack identification documents required by the Kenyan national identity system.²⁹⁵

69. Authentication failures can lead to exclusion from access to goods and services that are made conditional on successful authentication. Individuals who are excluded may consequently suffer disproportionate restrictions on their social and economic rights, including, but not limited to, the right to social security; the right to an adequate standard of living; the right to enjoyment of the highest attainable standard of physical and mental health; and the right to education.²⁹⁶

- a) The dissent of the Indian Supreme Court holds that proven authentication failures of biometric identity systems lead to exclusion of genuine and eligible beneficiaries.²⁹⁷ For example, the figures from the Economic Survey of India, an official document of the Government, indicated that there are millions of eligible beneficiaries across India who have suffered financial exclusion.²⁹⁸

293 Jean Drèze, "Dark clouds over the PDS," *The Hindu* (10 September 2016), <https://www.thehindu.com/opinion/lead/Dark-clouds-over-the-PDS/article14631030.ece>

294 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press, 2018).

295 See *Huduma Namba Judgment*, ¶¶ 1006, 1012.

296 International Covenant on Economic, Social and Cultural Rights, Arts. 9, 11, 12 and 13.

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

298 *Aadhaar Judgment*, ¶ 264 of dissent.

- b) The dissent of the Indian Supreme Court holds that the rights of individuals cannot be subject to probabilities, algorithms, and the “vicissitudes of technology.”²⁹⁹
- c) The dissent of the Indian Supreme Court holds that there can be no scope for any error in basic entitlements such as food, the lack of which can lead to malnutrition, destitution, and death.³⁰⁰
- d) The Indian Supreme Court holds that Aadhaar cannot be made mandatory for admission to schools because the right to education is a fundamental right of children and not a service, subsidy, or benefit under the Aadhaar Act.³⁰¹
- e) Exclusion is only amplified when there is function creep. The dissent of the Indian Supreme Court points out that the requirement of mandatory proof of possession of an Aadhaar number or requiring authentication had extended to 252 schemes at the time of writing the judgment in September 2018, including schemes relating to the rehabilitation of bonded labour, access to tuberculosis care, stipends for internships to students, and painting and essay competitions for children. Thus, citizens are denied not only basic services, but the wide range of services mandated by Aadhaar as a result of authentication failures.
- f) The dissent of the Indian Supreme Court cites Privacy International’s report on biometrics³⁰², which states that the varying accuracy and failure rates of biometric technology underlying identity systems can lead to misidentification, fraud, and civic exclusion.³⁰³

²⁹⁹ *Aadhaar Judgment*, ¶ 269 of dissent.

³⁰⁰ *Aadhaar Judgment*, ¶ 263 of dissent.

³⁰¹ *Aadhaar Judgment*, ¶ 332 at 401–402.

³⁰² Privacy International, *Biometrics: friend or foe of privacy?*, December 2013.
<https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy>

³⁰³ *Aadhaar Judgment*, ¶ 120 of dissent.

- g) The dissent of the Indian Supreme Court also cites several other research studies conducted by the state governments, academicians, and members of civil society in India documenting evidence of authentication failures, leading to exclusion and serious human rights violations.³⁰⁴
- h) The Kenyan High Court notes the risk of exclusion from access to goods and services that can result from both authentication failures and initial denial of enrolment because of a lack of documentation.³⁰⁵ The court finds that there is a need for a clear regulatory framework addressing potential exclusion.³⁰⁶

³⁰⁴ *Aadhaar Judgment*, ¶ 265–268 of dissent.

³⁰⁵ *Huduma Namba Judgment*, ¶¶ 876, 1012.

³⁰⁶ *Huduma Namba Judgment*, ¶ 1012.

RIGHTS OF THE CHILDREN

70. As noted elsewhere, there has also been consideration given to the rights of children and how they are impacted by identity systems particularly in relation to issues around consent and mission creep, as well as instances of discrimination and exclusion.

- a) The Jamaican Supreme Court states that the National Identification Registration Act (NIRA) affects the rights of children.³⁰⁷ Although the parent of the child must mandatorily apply for registration under the NIRA, there is no option for the child to opt out of the system if they wish to do so, completely taking away a child's control over their biometric information.³⁰⁸
- b) The Indian Supreme Court holds that while parents must consent on behalf of their children for enrolment in Aadhaar due to the inability of children to legally consent,³⁰⁹ once a child reaches the age of majority, they must be given the option to opt out of Aadhaar.³¹⁰
- c) The Kenyan High Court also notes that "special protection" must be given to children, because "they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."³¹¹ Due to this finding, the court determines that the legislative framework governing children's biometric data protection is inadequate.³¹²

³⁰⁷ *Julian J. Robinson*, ¶ 235.

³⁰⁸ *Julian J. Robinson*, ¶ 235.

³⁰⁹ *Aadhaar Judgment*, ¶ 332 at 401.

³¹⁰ *Aadhaar Judgment*, ¶ 332 at 401.

³¹¹ *Huduma Namba Judgment*, ¶ 820.

³¹² *Huduma Namba Judgment*, ¶ 823.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+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).