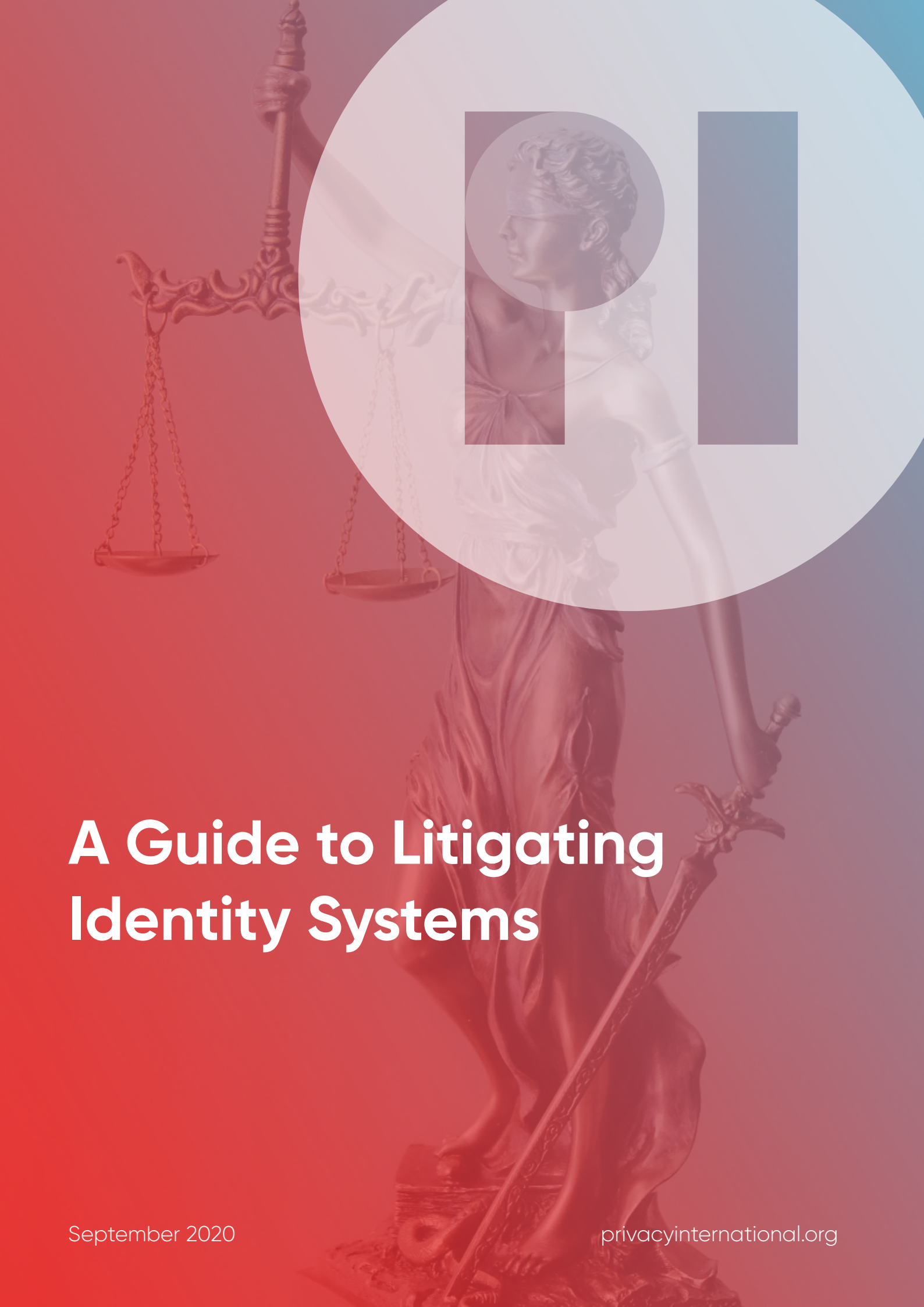

A Guide to Litigating Identity Systems

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

CONTENTS

EXECUTIVE SUMMARY

1. Some of the largest, data-intensive government programmes in the world are National Identity Systems – centralised government identity schemes that link an individual's identity to a card or number, often using biometric data and requiring identity authentication within the system for the provision of public benefits and participation in public life. The discussion surrounding these systems has largely centred on their perceived benefits for fraud protection, security, and the delivery of services. Although some national identity systems have been challenged in national courts, court analyses of the implications of identity systems have largely mirrored this broader public discourse centred on arguments in favour of identity systems. Two of the three most prominent national court judgments analysing identity systems – the *Aadhaar* judgment in India, the *Madhewoo* judgment in Mauritius, and the *Huduma Namba* judgment in Kenya – upheld the systems, lauding perceived benefits while under-developing critiques. Human rights advocates may find this largely one-sided discussion discouraging, as it limits the extent to which groups and individuals concerned about the human rights impact of identity systems can organise around strong arguments challenging those systems, in whole or part.
2. This argumentation guide seeks to fill that gap by providing a clear, centralised source of arguments advanced in and discussed by national courts that review the negative implications of identity systems, particularly on human rights. It gives advocates a tool for developing arguments in any given national context challenging an identity system, informing debate from a human rights perspective, and further building the repertoire of arguments that can be advanced in the future. The purpose of this guide is not to comprehensively describe the human rights implications of identity systems, or weigh identity systems' benefits against their disadvantages. While identity systems can have positive effects on human rights – helping to secure the right to a legal identity being the most obvious example – these aspects have been set out extensively in other spaces. This guide illuminates

the other side of the coin. The arguments against identity systems are still developing, and this guide therefore does not provide a comprehensive list of every possible argument. It does, however, provide an organised list of arguments against identity systems that can be read all together or separately, with a variety of reframed arguments meant to illustrate different approaches to challenging identity systems while relying on the same precedents.

3. This guide proceeds in five parts. First, the guide lays out the wide range of arguments challenging identity systems because of their impact on the right to privacy, providing advocates with tools for ensuring privacy right infringement is given adequate weight in courts' proportionality analyses. Second, it outlines arguments surrounding biometric information (which includes iris and fingerprint information), an important component of most identity systems, challenging assumptions of biometric authentication's effectiveness and necessity. Third, the guide presents arguments on data protection concerns, highlighting the importance of safeguards to protect rights and pointing to issues around the role of consent, function creep, and data sharing. Fourth, the guide sets out arguments on rights other than privacy, namely liberty, dignity, and equality. The fourth section provides detail on the social and economic exclusion and discrimination that can result from the design or implementation of identity systems.

4. Finally, the fifth section of this guide discusses identity systems' implications for the rule of law, the role of international human rights law, and considerations of gender identity. Rather than providing a list of arguments, as is the case in the other sections of this guide, the fifth section provides a general overview describing the absence of consideration of these themes in existing jurisprudence and the reasons why these themes warrant future consideration. By developing these arguments in conjunction with the variety of existing arguments illustrated in this guide, advocates can address and challenge the multitude of facets of human rights threatened by identity systems.

INTRODUCTION

5. The systems that states put in place to identify citizens and non-citizens bring with them great risks. This is particularly the case when they involve biometrics – the physical characteristics of a person, like fingerprints, iris scans, and facial photographs. While many countries in the world have existing ID cards, of varying types and prevalence, there has been a new wave in recent years of state "digital identity" initiatives. Most famous and largest of these is India's Aadhaar scheme, with over 1.2 billion people enrolled, their biometrics stored, and a unique 12-digit number issued, which is used for everything from receiving government benefits to opening a bank account.

6. However, these systems come with risks. There is a risk of exclusion, particularly for groups who have a history of being excluded or denied rights or citizenship. With digital identities being used more broadly, from accessing government subsidies through to education and health, the impact of exclusion is often worsened by these systems. Similarly, they create danger of exploitation by the state or the private sector by linking all stored data about a person back to a single number. The possibilities for surveillance, based on this 360-degree view of the person, are chilling.

7. Despite these dangers, affected individuals and communities are rarely consulted prior to these systems being introduced. Often identification systems are pushed through by decree, diktat, or means that allow less democratic accountability, denying the systems a democratic mandate and often a legal basis under the rule of law. The absence of such an inclusive, transparent legislative process means that there is no space to review, assess, and amend proposals before implementation. For something as intrinsically personal as identity, and with identity systems so open to potential abuse, the lack of democratic debate and accountability is concerning.

8. Activists and civil society organisations around the globe have been engaging with and critiquing these systems as they emerge. Sometimes, these have reached court to challenge the constitutionality of these systems and how they interfere with human rights, including privacy. In the last few years, civil society organisations from diverse disciplines and regions across the world have played key roles in these cases.

9. It is thanks to their tireless efforts that this guide exists, and we are honoured to have had the opportunity to give recognition and respect to the ground breaking work they have each undertaken to protect people and their dignity.

10. Privacy International has partnered with the International Human Rights Clinic at Harvard Law School to guide the reader through a simple presentation of the legal arguments explored by national courts around the world who have been tasked with discussing the negative implications of identity systems, particularly on human rights, and to present their judgment.

11. This initiative is part of our efforts, with our global partners, to ensure civil society and legal experts have access to the financial and technical resources they need to challenge these systems. This may include challenging the underlying assumptions behind identity systems, the global ecosystem pushing for their introduction, or demanding the necessary safeguards for privacy and other rights around identification systems, including scrutiny of the socio-economic, political, and legal state of deployment.

12. For too long, civil society organisations have been excluded from the development of identity systems, with their contribution limited to 'stakeholder engagement' sessions long after the important decisions have already been made. The expertise of these organisations has been downplayed, and the international debate dominated by players including governments, development banks, funding institutions, and management-consultant firms. The cases outlined in this guide prove that the knowledge and expertise of civil society organisations is huge: not only the impact of these systems on the people with which they work, but also the technical,

legal, and human rights implications. Going forward, these voices must be listened to and their expertise recognised in all debates on these topics. The voices of the real identity experts have been ignored for far too long, and it is time they are brought to the fore.

BACKGROUND TO THE NATIONAL COURT DECISIONS

13. The following paragraphs provide brief overviews of the three most recent and relevant identity systems cases. This line of cases from Mauritius, India, Jamaica, and Kenya inform the recent debate surrounding identity systems and the arguments discussed in this guide. Although other national cases exist and are mentioned throughout this guide, including cases in Taiwan and the Philippines, the Mauritian, Indian, Jamaican, and Kenyan judgments develop the core arguments illustrated here. While some international court judgments have explored biometrics, there has been a lack of identity systems jurisprudence at the international and regional court level thus far. Where identity systems have been discussed, national courts have generally acknowledged potential human rights implications, followed by some form of proportionality analysis weighing the rights implications with the stated aims and benefits of the systems. The balancing undertaken in these proportionality tests is highly court and context specific, but this guide provides a variety of arguments and potential rights implications that should be considered in light of proportionality frameworks.

MADHEWOO V. THE STATE OF MAURITIUS AND ANOR

14. The first case in the recent line of national identity systems cases is *Madhewoo v. The State of Mauritius and Anor*.[1] This case, decided by the Mauritian Supreme Court in 2015, upheld the collection of fingerprint data as part of a national identity card scheme, but rejected a centralised database for the storage of this data in the system.[2] The Mauritian court found that privacy rights guaranteed by the Mauritian Constitution's provisions governing searches were implicated by the system.[3] With respect to the collection of fingerprints, the court found that the potential infringement was outweighed by the interests in avoiding identity fraud furthered by the scheme.[4] In relation to the storage of fingerprint data, however, the court found that the lack of protections and judicial oversight in the proposed system outweighed the benefits of the storage regime.[5] At the conclusion of the Supreme Court's review, the Mauritian national identity system therefore consists of a mandatory identity card scheme where fingerprints are collected only for the initial verification of a cardholder's identity when the card is issued. The fingerprint data is not retained in a central database after that point, but the cards are required for the use of public services. The case was appealed to the Privy Council in 2016, but the Council upheld the Supreme Court's judgment and supported its reasoning.[6]

---

1 *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**

2 *Madhewoo,* 2015 SCJ 177 at 28, 34.

3 *Madhewoo*, 2015 SCJ 177 at 23.

4 *Madhewoo*, 2015 SCJ 177 at 28.

5 *Madhewoo*, 2015 SCJ 177 at 34.

6 *Madhewoo* v. The State of Mauritius and another, 2016 Privy Council No. 0006 .

JUSTICE K.S. PUTTASWAMY AND ANOTHER V. UNION OF INDIA AND OTHERS

15. The second case, and the most well-known, is the 2017 *Aadhaar* judgment from the Indian Supreme Court.[7] The Aadhaar system is a massive identity system that incorporates iris scans, fingerprint data, and a unique identity number, requiring enrolment for access to a wide variety of government programmes and schemes.[8] The judgment produced by the challenge to the system in 2017 included both the majority opinion that largely upheld the system and a dissenting opinion that strongly rejected the system's constitutionality. Unlike the Mauritian judgment, which focused almost exclusively on right to privacy concerns, the Indian Supreme Court opinions developed other rights arguments relating to exclusion. The majority in the *Aadhaar* case upheld the system, finding potential privacy violations and exclusionary impacts of the system to be outweighed by the extension of identity to marginalised communities and the state's interest in fighting corruption.[9] The dissenting opinion rejected the system, arguing that infringement of the right to privacy and exclusionary impacts could not be overcome simply because the system was used to address other basic human needs.[10] In the *Aadhaar* judgment, a number of other related issues are discussed, including the system's potential exploitation for mass surveillance, the democratic processes through which it was established, and the possible spread of the system throughout public and private life. The majority and dissent occasionally find common ground, including judicial

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

8 *Aadhaar Judgment*, ¶ 446 at 524.

9 *Aadhaar Judgment*, ¶ 308 at 376.

10 *Aadhaar Judgment*, ¶ 254 of dissent.

remedies and limiting function creep, that provides a variety of arguments useful for challenging identity systems.

JULIAN J. ROBINSON V. THE ATTORNEY GENERAL OF JAMAICA

16. The third case is *Julian J. Robinson v. The Attorney General of Jamaica* from 2019.[11] The proposed Jamaican identity system would have required the collection of biometric data from all Jamaican citizens and those residing in Jamaica for more than six months.[12] Those individuals would then be issued a unique identity number, with verification of the number required for the provision of any public goods or services and even some private services.[13] The Jamaican judgment was delivered in three opinions written by Justice Sykes, Justice Batts, and Justice Palmer Hamilton, with the Jamaican Supreme Court ultimately rejecting a proposed identity system. The court found the dissent from *Aadhaar* particularly persuasive, using its reasoning to find that privacy rights violations implicated by a compulsory identity scheme could not be justified by the system's potential benefits.[14] The court also found that the Jamaican system was unconstitutional because of a violation of the right to equality, as foreign nationals in Jamaica would not be subject to the identity system requirements.[15]

---

11 Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788 (2019).

12 *Julian J. Robinson*, ¶ 31.

13 *Julian J. Robinson*, ¶ 31.

14 *Julian J. Robinson*, ¶ 247 (B)(52).

15 *Julian J. Robinson*, ¶ 247 (A)(16).

NUBIAN RIGHTS FORUM AND OTHERS V. THE HON. ATTORNEY GENERAL

17. The fourth and most recent case is the *Huduma Namba* judgement from Kenya in 2020.[16] The proposed national identity system would have issued a national identity number to enrollees in Kenya, and the system would have centralised both biometric and other personal identity information – including DNA information and GPS coordinates – in a single national database.[17] The resulting national identity number would be used for access to services.[18] The Kenyan judgment ultimately upheld the system,[19] but the Kenyan High Court restrained the implementation of the system by requiring further data protection safeguards,[20] prohibiting the collection of DNA and GPS data,[21] and suggesting that potential exclusion from access to services and enrolment must be addressed.[22] In reaching its findings, the court took notice of the risks posed by collecting biometric information,[23] the potential for data abuse and misuse inherent to the system,[24] and the possibility of exclusion for vulnerable populations.[25]

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

17 *Huduma Namba Judgment*, ¶¶ 3–4.

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

19 *Huduma Namba Judgment*, ¶ 1047.

20 *Huduma Namba Judgment*, ¶ 922.

21 *Huduma Namba Judgment*, ¶¶ 767–68.

22 *Huduma Namba Judgment*, ¶ 1012.

23 *Huduma Namba Judgment*, ¶ 772.

24 *Huduma Namba Judgment*, ¶ 880.

25 *Huduma Namba Judgment*, ¶¶ 1012.

JUDICIAL YUAN INTERPRETATION NO. 603 AND BLAS F. OPLE V. RUBEN TORRES AND OTHERS

18. The other two national court judgments referenced throughout this guide are *Judicial Yuan Interpretation No. 603*[26] decided by the Judicial Yuan of Taiwan in 2005 and *Blas F. Ople v. Ruben Torres and others*[27] decided by the Supreme Court of the Philippines in 1998. In both instances, the courts – the highest in each respective jurisdiction – rejected proposed national identity systems because of privacy concerns.[28] The proposed systems would have linked national identity cards with the provision of public services.[29] Although the two judgments are shorter and less comprehensive than the more recent judgments, they provide additional useful support for several of the arguments developed in this guide.

19. Thus far, there has been little engagement with national identity systems by international and regional courts. Despite the inclusion of impacted rights in international human rights treaties (which are also referenced sparingly in national court judgments), there are no judgments evaluating the implications of national identity systems under the international human rights framework. Nevertheless, some relevant jurisprudence does exist for understanding the implications of biometrics more generally, including the European Court of Justice decision in *Michael Schwarz v. Stadt Bochum*[30] from 2013. In that case, the court reviewed the requirement of collection of

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

27 *Blas F. Ople* v. Ruben Torres and others, Supreme Court of the Republic of the Philippines, G.R. No. 127685 (1998).

28 See *Judicial Yuan Interpretation*; *Blas F. Ople*, Part III at 5.

29 *See Judicial Yuan Interpretation; Blas F. Ople*, Part III at 5.

30 *Michael Schwarz* v. Stadt Bochum, ECJ C-291/12 (2013).

fingerprint data for the issuance of passports in the EU, ultimately upholding the practice.[31]

20. In each of the national court judgments exploring the constitutionality of national identity systems, some form of proportionality test has been applied. In Kenya, a proportionality framework is outlined by the Kenyan High Court, although the judgment does not explicitly tie its findings to the framework. In Mauritius, the test was used in the specific context of a public order exception within the Mauritian Constitution's provisions governing searches. In India and Jamaica, the proportionality framework was employed to balance the negative consequences for human rights identified by the courts with the stated aims of the systems. Generally speaking, proportionality requires that a law or regulation: (1) have a legitimate state aim, (2) meet some threshold of substantial relationship to the stated aim, (3) meet some threshold of necessity for meeting the stated aim in the least restrictive way, and (4) balance in favour of the aim rather than the negative implications.[32] The various court judgments discussed in this guide differ in some respects in their conception of the proportionality requirements and their application to identity systems, but proportionality has formed the standard test under which these schemes are considered.

31 *Michael Schwarz*, ¶ 66.

32 See, eg *Madhewoo*, 2015 SCJ 177 at 27; *Aadhaar Judgment*, ¶ 446 at 540; *Aadhaar Judgment*, ¶ 218 of dissent; *Julian J. Robinson*, ¶ 247 (B)(19).

PART ONE:

THE RIGHT TO PRIVACY AND NATIONAL IDENTITY SYSTEMS

21. A common theme of all major pieces of national jurisprudence analysing the rights implications of national identity system is an analysis of the systems' impacts on the right to privacy.[33] As articulated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, the right to privacy is a fundamental right that protects individuals from arbitrary interferences with their privacy, family, home, and correspondence.[34]

22. The right to privacy is also enshrined in various other regional human rights instruments, including the European Convention on Human Rights, the American Convention on Human Rights, the Arab Charter on Human rights, and the Association of Southeast Asian Nations Human Rights Declaration. Furthermore, at a national level over 130 countries have constitutional statements regarding the protection of privacy.[35]

---

33 See, eg 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 23; Aadhaar Judgment, Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & connected matters, ¶ 29 of dissent (2018); *Opinion of Justice Sykes*, Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 174 (2019).

34 Privacy International, *What is Privacy?*, **https://privacyinternational.org/explainer/56/what-privacy** (retrieved 19 December 2019).

35 Privacy International, *What is Privacy?*

23. Privacy establishes "boundaries to limit who has access to our bodies, places and things, as well as our communications and our information."[36] The right to privacy is conceived differently in many national contexts, but it can include such themes as physical privacy, informational privacy, and autonomy.[37]

24. The right to privacy is a fundamental right that enables other rights. A key aspect of it, which is increasingly relevant to people's lives, is the protection of individuals' personal data. As early as 1988, the UN Human Rights Committee, recognised the need for data protection laws to safeguard the fundamental right to privacy.[38] In 2011, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued a report noting: "the protection of personal data represents a special form of respect for the right to privacy."[39]

25. While the right to data protection can be inferred from the general right to privacy, some international and regional instruments also stipulate a more specific right to protection of personal data, including the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[40]; the Council of Europe Convention 108 for the Protection of Individuals with Regard to the Processing of Personal Data[41]; the EU Charter of Fundamental Rights; the EU General Data Protection Regulation[42]; the Asia–Pacific Economic Cooperation Privacy Framework 2004[43]; and the Economic Community of

---

36 Privacy International, *What is Privacy?*

37 See, eg Madhewoo, 2015 SCJ 177 at 23; Aadhaar Judgment, ¶ 29 of dissent; *Opinion of Justice Sykes*, ¶ 174.

38 UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), ¶ 10.

39 UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 16 May 2011, UN Doc. A/HRC/17/27, ¶ 58.

40 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, **https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm**

41 Council of Europe, *Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data,* **https://www.coe.int/en/web/data-protection/convention108-and-protocol**

42 European Commission, General Data Protection Regulation, **https://gdpr-info.eu/**

43 Asia–Pacific Economic Cooperation, *APEC Privacy Framework*, **www.apec.org**

West African States Supplementary Act on Personal Data Protection[44] from 2010. As of 2019, over 130 countries now have some form of privacy and data protection law, and another 40 countries have pending bills.[45]

26. As the right to privacy is a qualified right, human rights instruments that guarantee the right to privacy and the protection of individuals' personal data may sometimes permit interferences with these rights if they abide by certain principles, such as legality, necessity, and proportionality, and do not interfere with the essence of those rights.[46]

27. In other words, as affirmed also by the UN Human Rights Committee, ensuring that any interference with the right to privacy is not arbitrary or unlawful requires a two-part test: (1) legality and (2) necessity and proportionality. The first part of the test means that any interferences with privacy can only take place "in cases envisaged by the law." Second, states must demonstrate that the interference must "proportionate to the end sought, and … necessary in the circumstances of any given case."[47]

28. However, there are limits to the extent of permissible interference with a Covenant right. As the UN Human Rights Committee has emphasised: "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."[48] The UN High Commissioner for Human Rights has similarly observed that "any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights."[49]

---

44 Economic Community of West African States (ECOWAS), Supplementary Act on Personal Data Protection within ECOWAS, **http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf**

45 See David Banisar, *National Comprehensive Data Protection/Privacy Laws and Bills 2019*, last revised 5 December 2019, **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416** (retrieved 23 July 2020).

46 See, among others, International Covenant on Civil and Political Rights, Article 17(1) ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation").

47 *UN Human Rights Committee*, ¶¶ 3 and 8.

48 *UN Human Rights Committee*, General Comment 27 and General Comment 31.

49 UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/27/37, 30 June 2014, ¶ 23.

29. The use of any data by the state, including the implementation of an identity system, must be carried out against this backdrop with respect for all fundamental human rights. The collection of data to be used in the system and the storage of data can both independently implicate privacy rights and involve overlapping and distinct considerations. Additionally, the particular risks associated with identity systems – heightened danger of cybersecurity attacks,[50] identity fraud,[51] and potential facilitation of mass surveillance[52] – further threaten the right to privacy. Given these risks to privacy, it is vital to ensure courts give adequate weight to potential privacy rights violations in their balancing of competing interests in order to prevent disproportionate or unnecessary impacts on privacy in furtherance of the stated aims of the systems.[53]

30. This section of the guide provides a variety of arguments explored by different jurisdictions, addressing different conceptions of privacy rights and balancing the importance of privacy rights with proposed benefits of identity systems. Advocates and human rights defenders should utilise this section of the guide to raise identity systems' impacts on privacy rights and challenge the systems under the proportionality frameworks used by courts to analyse the systems.

50 See *Madhewoo*, 2015 SCJ 177 at 30.

51 See *Opinion of Justice Sykes*, ¶ 54.

52 *Aadhaar Judgment*, ¶ 247 of dissent.

53 See *Aadhaar Judgment*, ¶ 254 of dissent.

IDENTITY SYSTEMS' IMPLICATIONS FOR THE RIGHT TO PRIVACY

31. National Identity Systems implicate all these components of privacy through the collection of biometric data, the use of biometric data for authentication,[54] the storage and sharing of sensitive personal information, including biometric data, in the system,[55] and the mandatory nature of national identity systems.[56]

Collection

32. The collection of biometric data and their use for authentication of an identity card interferes with the right to privacy because the physical process of obtaining biometric data like fingerprints and iris scans constitutes an invasion of an individual's physical person.

    a) The Mauritian Supreme Court relied on this framing of a potential violation of the right to privacy under its constitution when reasoning about the Mauritian national identity system.[57] 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 the Mauritian Constitution.[58] Although the court ultimately found that any infringement of the right to privacy was overcome by the public interest,[59] the case

54 See *Madhewoo*, 2015 SCJ 177 at 23.

55 See *Madhewoo*, 2015 SCJ 177 at 33.

56 See *Opinion of Justice Sykes*, ¶ 174.

57 *Madhewoo*, 2015 SCJ 177 at 23.

58 *Madhewoo*, 2015 SCJ 177 at 23.

59 *Madhewoo*, 2015 SCJ 177 at 28.

demonstrates an effective use of this argument to show an implication of the right to privacy.

b) The majority of the Indian Supreme Court does not discuss biometric data collection as a physical search, but the court does express the importance of the physical aspect of privacy in understanding the right to privacy.[60] Physical privacy of the person is conceived of as one of the three forms of privacy protected by the right to privacy.[61] Searches have jurisdictionally specific legal definitions, so although the Indian court does not engage in an analysis of biometric data collection as a search, that does not diminish the importance of the physical component of privacy. Rather, it means physical privacy is considered under a different legal framework – the right to privacy framework analysed in the *Aadhaar* judgment.

c) Justice Sykes of the Jamaican Supreme Court suggests that the compulsory taking of biometric data is a violation of the right to privacy of the person because human beings have an inherent right to bodily integrity[62] and because biometric data can reveal sensitive health information, such as an individual's specific medical conditions.[63]

33. The mandatory collection of personal data as part of an identity system implicates the right to privacy because it interferes with the informational privacy of the individual.

a) The dissenting opinion in the *Aadhaar* judgment references informational privacy specifically in its discussion of what it conceives as an unconstitutional violation of the right to privacy.[64] The dissent describes

60 See *Aadhaar Judgment*, ¶ 83 at 164.

61 *Aadhaar Judgment*, ¶ 232 at 302.

62 *Opinion of Justice Sykes*, ¶ 247(A)(10).

63 *Opinion of Justice Sykes*, ¶ 55.

64 *Aadhaar Judgment*, ¶ 31 of dissent.

informational privacy as "the right to an individual to disseminate certain personal information for limited purposes alone."[65]

b) The majority opinion in *Aadhaar* similarly focuses on the implication of the informational privacy component of the right to privacy in its own discussion of the right to privacy,[66] although the majority finds the interference with informational privacy to be proportional to the public benefit achieved by the system.[67] The majority describes informational privacy as privacy that "protects a person by giving her control over the dissemination of material that is personal to her and disallowing unauthorised use of such information by the State."[68]

c) Justice Sykes of the Supreme Court of Jamaica references informational privacy expressly in stating: "compulsory taking of any biometric data is a violation of the right to privacy – privacy of the person, informational privacy."[69]

d) The Kenyan High Court grounds its privacy right analysis in the concept of informational privacy.[70] The court describes informational privacy as "rights of control a person has over personal information," which "closely relates to the personal and is regarded as intimate, and which a person would want to restrict the collection, use and circulation thereof."[71] Building on this focus, the court finds that some types of personal data collected by the Kenyan national identity system – particularly DNA information and GPS coordinates – are "personal, sensitive and intrusive" and therefore require protection.[72]

---

65 *Aadhaar Judgment*, ¶ 29 of dissent.

66 See *Aadhaar Judgment*, ¶ 287 at 357.

67 *Aadhaar Judgment*, ¶ 308 at 376.

68 *Aadhaar Judgment*, ¶ 83 at 164.

69 *Opinion of Justice Sykes*, ¶ 247(A)(10).

70 See *Huduma Namba Judgment*, Nubian Rights Forum and Others v. The Hon. Attorney General, Consolidated Petitions No. 56, 58 & 59 of 2019 ¶ 750 (2020).

71 *Huduma Namba Judgment*, ¶ 750.

72 *Huduma Namba Judgment*, ¶ 772.

e) The Judicial Yuan of Taiwan identified the issuance of national identity cards incorporating fingerprints as implicating the right to informational privacy.[73]

f) The European Court of Justice identifies fingerprint data as unique personal data implicating the right to a private life (albeit not in the context of a challenge to an identity system).[74] The court's analysis focuses on the personal data protections necessary to ensuring the right to a private life,[75] a focus closely resembling informational privacy arguments employed by the other courts discussed earlier.

g) The European Court of Human Rights concluded that Article 8 of the European Convention on Fundamental Rights, ie the right to private life, family life, correspondence, and home, provided "for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged."[76]

34. The mandatory collection of personal data as part of an identity system interferes with the right to privacy because it interferes with an individual's autonomy and freedom of choice.

a) The majority opinion in the *Aadhaar* judgment focuses its proportionality around the idea that the identity system places personal autonomy at odds with the public interest.[77] The majority's conception of personal autonomy is "the free exercise of the will according to one's own values, interests, and desires."[78]

---

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

74 Michael Schwarz v. Stadt Bochum, ECJ C-291/12, ¶ 27–30 (2013).

75 See *Michael Schwarz*, ¶ 24–25.

76 Satakunnan Markkinapörssi Oy and Satamedia Oy V. Finland, Application No. 931/13, Judgment (Merits and Just Satisfaction), Grand Chamber, European Court of Human Rights, 27 June 2017.

77 See *Aadhaar Judgment*, ¶ 285 at 355.

78 *Aadhaar Judgment*, ¶ 116 at 199.

b) The dissenting opinion in the *Aadhaar* judgment finds a lack of consent in the identity system particularly troubling.[79] Consent is similar to the concept of personal autonomy that the majority focuses on because it directly involves an individual's freedom to choose to accept or reject participation in the identity system in accordance with their values, interests, and desires. Ignoring or minimising the importance of consent therefore undermines personal autonomy and the freedom of choice.

c) Justice Sykes of the Jamaican Supreme Court states the privacy of choice has been removed by the compulsory nature of the identity system reviewed in that case.[80] Justice Sykes conceives of the freedom of choice as privacy protecting "an individual's autonomy over fundamental personal choices."[81]

d) The Kenyan High Court cites the ability to collect and match an individual's biometric characteristics without their personal knowledge or consent in determining that DNA information should warrant protection.[82] Additionally, the court's conception of informational privacy, which it uses as its underlying basis in evaluating the Kenyan national identity system's privacy implications, includes in its definition an element of control.[83]

35. The collection of personal data as part of an identity system is a disproportionate interference with the right to privacy because it enhances the state's ability to engage in mass surveillance, or the systematic monitoring and tracking of all individuals enrolled in the identity system.

a) The dissenting opinion in the *Aadhaar* judgment notes the danger posed by an identity system with respect to mass surveillance, observing that identity systems increase the potential for building comprehensive profiles

79 *Aadhaar Judgment*, ¶ 304 of dissent.

80 *Opinion of Justice Sykes*, ¶ 247(A)(10).

81 *Opinion of Justice Sykes*, ¶ 174.

82 *Huduma Namba Judgment*, ¶ 767.

83 See *Huduma Namba Judgment*, ¶ 750 (referring to informational privacy as "rights of control a person has over personal information").

of individuals.[84] The dissent states: "biometric data not only allows individuals to be tracked, but it also creates the potential for the collection of an individual's information and its incorporation into a comprehensive profile."[85]

b) The majority opinion in the *Aadhaar* judgment ultimately rejects mass surveillance concerns because of oversight by the Technology and Architecture Review Board and Security Review Committee (government committees established by the Aadhaar legislation) and prohibitions on the recording of information about the nature of the transaction, encryption, and data silos.[86] However, the court does not make this determination concerning identity schemes generally, but instead relies on data minimisation and anonymity within the Aadhaar system.[87] Data minimisation means the collection and storage of only minimal data necessary for effective authentication, including prohibition on the collection of data unrelated to the purpose of the transaction.[88]

c) Justice Sykes of the Jamaican Supreme Court references the danger of power afforded to the state by the linking of data across state databases under the Jamaican identity system.[89] Linking databases together allows individuals to be tracked and provides the state with the ability to build a comprehensive profile of an individual.[90]

d) Justice Batts of the Jamaican Supreme Court holds that the Jamaican identity system implicates a danger of abuse by the state and its

84 *Aadhaar Judgment*, ¶ 239 of dissent.

85 *Aadhaar Judgment*, ¶ 239 of dissent.

86 *Aadhaar Judgment*, ¶ 447 at 541–544.

87 See *Aadhaar Judgment*, ¶ 208 at 285.

88 See *Aadhaar Judgment*, ¶ 191–95 at 271–274.

89 *Opinion of Justice Sykes*, ¶ 246.

90 *Opinion of Justice Sykes*, ¶ 246.

agencies, particularly where affected persons are not afforded the right to be heard.[91]

e) The Supreme Court of the Philippines has noted the risk that a biometric identity system could be used for nefarious state surveillance activities, such as tracking an individual's movements, or evading constitutional search and seizure protections by accessing an individual's information via the identity system database.[92]

Storage

36. The centralised storage of biometric data for authentication in an identity system (the process whereby an individual's identity is verified by matching their biometric data at the point of authentication with the data stored in the identity system's database) constitutes a disproportionate interference with the right to privacy because it heightens the risk of cybersecurity breaches.

a) The Mauritian Supreme Court rejects the centralised, indefinite storage of fingerprint data largely by focusing on the risk of security breaches that were not adequately defended against.[93] Specific security breach risks identified by the court included: cloning government credentials and using them to access the database; an indirect proxy attack on the database via the government's portal; accessing data on the local machines used to upload data to the database server; and reading data from identity cards at a distance with special devices.[94]

---

91 *Opinion of Justice Batts*, Julian J. Robinson v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 349, 366 (2019).

92 *Blas F. Ople* v. Ruben Torres and others, Supreme Court of the Republic of the Philippines, G.R. No. 127685, Part III at 5 (1998).

93 *Madhewoo*, 2015 SCJ 177 at 30–32.

94 *Madhewoo,* 2015 SCJ 177 at 30.

b) The dissenting opinion in the *Aadhaar* judgment identifies a risk that a nationalised, centralised database incorporated into an identity system could be prone to cybersecurity threats because adversaries of the state have an interest in inflicting damage on individuals' biometric credentials when they are seeded across an entire identity system, as well as threats caused by market incentives for public and private organisations with access to the system to sell individuals' personal data.[95]

c) Justice Sykes of the Jamaican Supreme Court refers to concerns that data stored as part of the identity system could fall into the hands of third parties, which could expose sensitive information like medical data.[96] Justice Sykes identifies specific threats of attack to the system as including Trojan Horse attacks and spoofing attacks.[97]

d) The Kenyan High Court argues that there will be risks of "attacks or unauthorised access" with "any storage" of personal data, but acknowledges that centralised storage affords data subjects less information and control over their data's use.[98] In light of the risk of attack or unauthorised access of biometric data stored in either a centralised or decentralised system, the court concludes that strong security policies are required if systems are to comply with international data protection standards – a requirement the court imposes on the Kenyan national identity system.[99]

95 *Aadhaar Judgment*, ¶ 245 of dissent.

96 *Opinion of Justice Sykes*, ¶ 55.

97 *Opinion of Justice Sykes*, ¶ 54.

98 *Huduma Namba Judgment*, ¶ 880.

99 *Huduma Namba Judgment*, ¶ 883.

e) The majority opinion in the *Aadhaar* judgment is significantly less concerned with security risks, partly because of the offline storage used in the Aadhaar system.[100] The majority also highlights the potential data protection law[101] and limits the length of time for which data can be stored. The majority found the time period to be unreasonable and too great a risk to an individual's right to be forgotten.[102]

f) The Supreme Court of the Philippines identified a risk that, in the event of a security breach, an intruder could access or manipulate the information stored in an identity system, leading to exposure or alteration of an individual's loan availments, income tax returns, and documents regarding sensitive medical information.[103]

37. The storage of biometric data for authentication in an identity interferes with the right to privacy because the data is permanent, and its collection and storage inhibits an individual's ability to be forgotten.

a) The majority opinion in the *Aadhaar* judgment discusses the right to be forgotten,[104] although it ultimately finds the identity system to be constitutionally permissible.[105] The majority conceives of the right to be forgotten as the "right to prevent or restrict disclosure of personal data by a fiduciary."[106]

b) Influential scholarly sources for the dissenting opinion in the *Aadhaar* judgment argue that biometric data collection specifically implicates the right to remain anonymous.[107] Anonymity is inextricably associated with the right to privacy as an individual cannot have a reasonable expectation that

100 *Aadhaar Judgment*, ¶ 48 at 57.

101 *Aadhaar Judgment*, ¶ 225 at 298.

102 *Aadhaar Judgment*, ¶ 205 at 283.

103 *Blas F. Ople*, Part III at 5.

104 *Aadhaar Judgment*, ¶ 205 at 282.

105 *Aadhaar Judgment*, ¶ 308 at 376.

106 *Aadhaar Judgment*, ¶ 225 at 298.

107 *Aadhaar Judgment*, ¶ 127 of dissent.

their privacy is being protected without the ability to control what information is shared about them and how that information is used, and what information is used to identify them.

c) Justice Sykes of the Jamaican Supreme Court identifies the right to anonymity to be an important component of the right to privacy when discussing the Jamaican identity system.[108]

38. The storage of biometric data for authentication in an identity system amounts to an interference with the right to privacy because it increases the risk of identity theft, in which the information necessary for using another individual's legal identity is stolen and is used to further access other personal information or use services and benefits in another person's name.

a) The Mauritian Supreme Court rejected the indefinite storage of fingerprint data in a centralised register, partly for fear that data could be stolen from identity cards.[109] The data necessary for identity theft could be obtained through a variety of hacking attacks, from cloning government credentials for access to the system, engaging in a proxy attack via the government's portal to the database, or taking data from the local machines used to upload data to the centralised register.[110] A centralised database, which can never be foolproof, can expose all data stored on the database in the event its security is compromised.[111]

b) Justice Sykes of the Jamaican Supreme Court refers to concerns that data stored as part of the identity system could fall into the hands of third parties, including hackers using Trojan Horse or spoofing attacks on the database and exposing an individual's sensitive data like medical information.[112]

---

108 *Opinion of Justice Sykes*, ¶ 247(A)(11).

109 *Madhewoo,* 2015 SCJ 177 at 30.

110 *Madhewoo* 2015 SCJ 177 at 30.

111 See *Madhewoo,* 2015 SCJ 177 at 30.

112 *Opinion of Justice Sykes*, ¶ 54.

c) The Kenyan High Court explicitly references the risk of identity theft as a form of misuse or unauthorised access, giving rise to the data protection requirements the court imposes on the Kenya national identity system.[113]

d) The Kenyan High Court prohibits the collection of GPS coordinates as part of the national identity system, referencing the ability to use such data to "track and monitor people without their knowledge."[114] The other form of data prohibited by the court – DNA information – could similarly be used for "negative profiling of individuals for ulterior motives."[115]

39. The storage of biometric data constitutes a disproportionate interference with the right to privacy because it increases the state's ability to engage in mass surveillance.

a) The Mauritian Supreme Court rejects the centralised storage of fingerprint data partly because of the ease of access to data by state actors without judicial oversight.[116] The court states that judicial oversight over interference with the legal and constitutional rights of citizens is a "fundamental principle of the rule of law" and its absence is "inconceivable."[117]

b) The majority in the *Aadhaar* judgment rejects mass surveillance concerns by relying partly on the use of data silos in the system to prevent improper access of data outside the Aadhaar scheme's purpose.[118] Data silos are collections of information within the system that are isolated from and inaccessible to other parts of the system.[119]

---

113 *Huduma Namba Judgment*, ¶ 880.

114 *Huduma Namba Judgment*, ¶ 768.

115 *Huduma Namba Judgment*, ¶ 767.

116 *Madhewoo,* 2015 SCJ 177 at 33.

117 *Madhewoo,* 2015 SCJ 177 at 33.

118 See *Aadhaar Judgment*, ¶ 208 at 285.

119 See Garrett Alley, "What are data silos," *Alooma* (20 December 2018) at **https://www.alooma.com/blog/what-are-data-silos**

c) The dissent in the *Aadhaar* judgment highlights the ability of the state to create comprehensive individual profiles based on data linked across databases used by the identity system.[120] Individual profiles increase the state's ability to track an individual's movements and can fix permanent stigma to an individual's identity in the system.[121]

d) The Kenyan High Court explicitly references profiling and surveillance as forms of potential misuse or unauthorised access, giving rise to the data protection requirements imposed by the court on the Kenyan national identity system.[122] Moreover, the court prohibits the collection of GPS coordinates as part of the national identity system, referencing the ability to use such data to "track and monitor people without their knowledge."[123] The court also finds that centralised databases storing GPS information could be used to "create 'watchlists' or 'blacklists'," thereby "leading to a reversal of the presumption of innocence."[124]

e) Justice Sykes of the Jamaican Supreme Court references the danger of power afforded to the state by the linking of data across state databases under the Jamaican identity system.[125] Justice Sykes quotes scholar Nancy Liu and states when "unique identification just from biometric data is combined with a unique identification number is seeded into multiple databases and the use of the unique number is tracked the 'biometric data not only allow individuals to be tracked, but create the potential for the collection of an individual's information and its incorporation into a comprehensive profile by linking various databases together.'"[126]

---

120 *Aadhaar Judgment*, ¶ 247 of dissent.

121 *Aadhaar Judgment*, ¶ 247 of dissent.

122 *Huduma Namba Judgment*, ¶ 880.

123 *Huduma Namba Judgment*, ¶ 768.

124 *Huduma Namba Judgment*, ¶ 918.

125 *Opinion of Justice Sykes*, ¶ 246.

126 *Opinion of Justice Sykes*, ¶ 246.

USES OF BIOMETRIC DATA: PROFILING

40. The use of biometric data in identity systems can lead to a disproportionate interference with the right to privacy because they help track the movement of people enrolled in the system and create comprehensive profiles of individuals.

    a) Justice Sykes of the Jamaican Supreme Court argues that the pairing of biometric data with a unique identification number allows the state to track individuals.[127] Justice Sykes also finds that the biometric data and unique identification number system envisioned in Jamaica would allow for profiling.[128] This is the case because the data seeded across databases for verification purposes can be linked and used to create a profile of an individual.[129]

    b) The Supreme Court of the Philippines identified the risk that an individual's movements could be tracked using a national identity system because the individual would need to present their identification whenever they dealt with a government agency, the instances of which will necessarily be recorded.[130] The court also suggests that the sophisticated data centre housing the information could then create a "cradle-to-grave dossier on an individual."[131]

127 *Opinion of Justice Sykes*, ¶ 246.

128 *Opinion of Justice Sykes*, ¶ 246.

129 *Opinion of Justice Sykes*, ¶ 246.

130 *Blas F. Ople*, Part III at 5.

131 *Blas F. Ople*, Part III at 5.

c) The dissenting opinion in the *Aadhaar* judgment also raises concerns of tracking, stating: "biometric data not only allows individuals to be tracked, but it also creates the potential for the collection of an individual's information and its incorporation into a comprehensive profile."[132]

d) The Kenyan High Court prohibits the collection of GPS coordinates in the Kenyan national identity system partly because the coordinates could be used to "track and monitor people without their knowledge."[133] The court also prohibits the collection of DNA information for use in the system, referencing the ability to use DNA and other biometric identifiers for "negative profiling of individuals for ulterior motives."[134]

e) The majority in the *Aadhaar* judgment is satisfied that exact information regarding the purpose of an authentication request is not stored in the Aadhaar system, but the majority also points out that some data regarding location is recorded.[135] The majority opinion in the *Aadhaar* judgment rejects profiling concerns, but relies on anonymisation, data minimisation, and the use of data silos to reach this conclusion.[136] If these facets of the system did not exist, the majority may not have reasoned as it did.

---

132 *Aadhaar Judgment*, ¶ 239 of dissent.

133 *Huduma Namba Judgment*, ¶ 768.

134 *Huduma Namba Judgment*, ¶ 767.

135 *Aadhaar Judgment*, ¶ 197 at 276.

136 *Aadhaar Judgment*, ¶ 208 at 285.

USES OF BIOMETRIC DATA: DATA SHARING WITH SECURITY AGENCIES

41. Identity systems can aid in mass surveillance because identity system data may be shared with or accessed by state security agencies, which amounts to a disproportionate interference with the right to privacy, and may also increase the risk of other human rights violations.

    a) The Mauritian Supreme Court noted its concern with the relative ease with which government, as well as private, actors could access fingerprint data stored in the Mauritian identity system.[137] In that system, for example, police would have been able to access identity system data for the very broad purposes of "the prevention or detection of crime, the apprehension or prosecution of offenders on the assessment or collection of any tax, duty or any imposition of a similar nature" without judicial oversight.[138]

    b) The majority opinion in the *Aadhaar* judgment finds issue with a provision of the Aadhaar system's legislation that allowed for the disclosure of data in the interest of national security, arguing that the provision would need to be changed by increasing the rank of security services officers who determine when data is to be shared and involving a judicial officer in the decision.[139]

137 *Madhewoo*, 2015 SCJ 177 at 33.

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

139 *Aadhaar Judgment*, ¶ 349 at 424.

c) Justice Batts of the Jamaican Supreme Court holds that the envisioned Jamaican identity system's mechanism for disclosure of data to police lacks adequate protections and safeguards.[140] Justice Batts would require any mechanism for disclosing data to security services to include an opportunity to be heard by the individual affected and a limitation on the time period for which data can be retained.[141]

140 *Opinion of Justice Batts*, ¶ 366.

141 *Opinion of Justice Batts*, ¶ 366.

NECESSITY AND PROPORTIONALITY TEST: THE CASE OF IDENTITY SYSTEMS

42. An identity system's infringement on privacy rights cannot be justified if unnecessary for or disproportionate to the benefits of the system. The UN High Commissioner of Human Rights recommends that states, inter alia, "ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim."[142]

43. This is emphasised in the UN General Assembly resolution on the right to privacy in the digital age: "Noting the increase in the collection of sensitive biometric information from individuals, and stressing that States must respect their human rights obligations and that business enterprises should respect the right to privacy and other human rights when collecting, processing, sharing and storing biometric information by, inter alia, considering the adoption of data protection policies and safeguards."[143]

    a) The dissent in the *Aadhaar* judgments finds that the Aadhaar system fails a proportionality test.[144] The dissent accepts the state's aim of effectively fulfilling its welfare programmes.[145] However, the dissent argues that the infringement of the privacy has not been shown to be necessary for effectuating that purpose.[146]

142 UN High Commissioner for Human Rights, Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, 3 August 2018, UN Doc. A/HRC/39/29.

143 UN General Assembly Resolution 73/179, 17 December 2018.

144 *Aadhaar Judgment*, ¶ 254 of dissent.

145 *Aadhaar Judgment*, ¶ 176 of dissent.

146 *Aadhaar Judgment*, ¶ 254 of dissent.

b) Justice Sykes of the Jamaican Supreme Court applies a proportionality framework in finding the Jamaican identity system unconstitutional.[147] Justice Sykes holds that the system fails to meet the necessity stage of this analysis,[148] while also determining that the interference with privacy is disproportionate to the system's objective of providing citizens with reliable identification.[149]

c) The Judicial Yuan of Taiwan found an absence of a close relationship between the collection of fingerprints and preventing the misuse of identity cards, as well as a failure to achieve a balance of losses to informational privacy to gains of effective identification when reviewing a proposed identity card system.[150]

44. Proportionality of an identity system's benefits and infringements on privacy cannot be satisfied unless sufficient data protection safeguards exist.

a) The dissent in the *Aadhaar* judgment explicitly envisions a requirement for sufficient safeguards and consent in outlining its proportionality test.[151] The failure to establish these safeguards is part of the dissent's argument against the constitutionality of the Aadhaar system.[152]

b) The Kenyan High Court states: "the lack of a comprehensive legal framework" for the protection of personal data collected as part of the national identity system "is contrary to the principles of democratic governance and the rule of law, and thereby unjustifiable."[153] The absence of appropriate data protection safeguards was one of the two privacy infringements analysed by the court under its purported proportionality

147 *Opinion of Justice Sykes*, ¶ 247(B)(4)–(5).

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

149 *Opinion of Justice Sykes*, ¶ 247(B)(19).

150 Judicial Yuan Interpretation No. 603, Taiwan, Reasoning (2005).

151 *Aadhaar Judgment*, ¶ 218 of dissent.

152 *Aadhaar Judgment*, ¶ 306 of dissent.

153 *Huduma Namba Judgment*, ¶ 922.

test,[154] although the court does not explicitly state what prong of the test failed due to the system's data protection deficiencies. The Kenyan High Court's assessment of the need for adequate data protection safeguards also ventures one step further, stating that even where a legal framework formally exists, the data protection requirement cannot be met without operationalisation and implementation of the legal framework.[155]

c) While the Mauritian court does not explicitly state this framework, the court finds the storage of fingerprint data used in its identity system to fail the public order exception test because of the lack of safeguards in the data protection regime.[156]

154 See *Huduma Namba Judgment*, ¶ 911.

155 *Huduma Namba Judgment*, ¶ 853.

156 *Madhewoo*, 2015 SCJ 177 at 30–32.

d) The Supreme Court of the Philippines did not employ a proportionality framework like this, but the court emphasised the absence of safeguards in finding that the state's objectives in instituting an identity system did not justify the system's infringement on privacy.[157] The Philippine court would require a compelling state interest and proper safeguards;[158] a similar but conceptually different standard.

45. The "bread v. freedom" argument, where derogations of individual rights are justified by improved access to basic needs, does not justify an identity system's infringement of the right to privacy because privacy rights and economic rights are not mutually exclusive. The state must protect both rights.

    a) The dissent in the *Aadhaar* judgment specifically makes this argument, finding that the state has failed to demonstrate why the Aadhaar system's benefits to the welfare scheme require the system's infringements on privacy.[159]

157 *Blas F. Ople*, Part III at 6.

158 *Blas F. Ople*, Part III at 6.

159 *Aadhaar Judgment*, ¶ 254 of dissent.

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.

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.

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 biometrics[277], 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 India[291] 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 immobilse 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 biometrics[302], 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.

PART FIVE:

PATHS FORWARD

DEMOCRACY, THE RULE OF LAW, AND ACCESS TO JUSTICE

71. This analysis of the jurisprudence on identity systems leads to the conclusion that the manner in which identity systems are introduced and designed poses serious threats to democracy, the rule of law, and access to justice. The Jamaican Supreme Court observed that governance in a constitutional democracy based on the rule of law is an institutional arrangement, with each arm performing its designated functions.[313] However, the adoption of identity systems is rarely preceded by rigorous legislative debates and democratic deliberation.[314]

72. According to the dissenting opinion in the *Aadhaar* judgment, the passing of the Aadhaar Act as a "Money" Bill was unconstitutional. Under the Articles of the Indian Constitution, a Money Bill is a category of bill (draft law) that contains provisions to deal with the specific list of matters such as the withdrawal of money from the Consolidated Fund of India and the regulation of taxes.[315] The dissent in the *Aadhaar* judgment held that the incorrect classification of the draft Aadhaar legislation as a Money Bill, amounted to "a

313 *Julian J. Robinson* v. The Attorney General of Jamaica, Claim No. 2018HCV01788, ¶ 167 (2019).

314 See Privacy International, The Clash between Democracy and Biometrics, 31 January 2018, **https://medium.com/@privacyint/identity-policies-the-clash-between-democracy-and-biometrics-95adabd9f263** (last visited 20 November 2019).

315 Article 110 of the Indian Constitution.

fraud on the constitution" because it led to the bypassing of the Upper House of the Parliament (Rajya Sabha) and undermined the constitutional scheme of bicameralism and the legitimacy of democratic institutions.[316] While this was the position adopted in the dissenting opinion of the *Aadhaar* judgment, it is pertinent to note that the Indian Supreme Court has, in a subsequent decision, questioned the majority's decision that Aadhaar was correctly certified as a Money Bill. The court referred the question of whether the Aadhaar Act was correctly certified as a Money Bill for reconsideration to a larger Bench of the Supreme Court.[317]

73. Petitioners in the Kenyan case similarly raised arguments regarding the lack of public participation in the legislation establishing the Kenyan national identity system, in particular the use of an omnibus bill that the Kenyan High Court previously cautioned against using for anything other than non-substantive amendments.[318] While the Kenyan court ultimately upheld the method used to introduce the legislation, this instance provides another example of the need for respect for democratic processes that allow for complete public participation in the design and implementation of proposed national identity systems. The rule of law and the proper functioning of democracies also depends on the efficient functioning of legal institutions to ensure access to justice for all.

74. 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. The Indian Supreme Court in the *Aadhaar* judgment found that Section 47 of the enacting legislation, which barred courts from admitting complaint in relation to the Aadhaar Act unless filed by the UIDAI (the statutory authority

316 Aadhaar Judgment, Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & connected matters, ¶ 117 of dissent (2018).

317 IndiaToday, "Supreme Court re-examines Aadhaar as money bill, refers issue to larger bench," 4 November 2019, **https://www.indiatoday.in/india/story/supreme-court-re-examines-aadhaar-as-money-bill-refers-issue-to-larger-bench-1618683-2019-11-14** (last visited 20 November 2019).

318 *Huduma Namba Judgment*, Nubian Rights Forum and Others v. The Hon. Attorney General, Consolidated Petitions No. 56, 58 & 59 of 2019 ¶ 676 (2020).

established under the legislation to implement the identity system) or a person authorised by it, was unconstitutional because it barred individual citizens from seeking judicial remedies for breach of data.[319] Similarly, the Mauritian Supreme Court rejected the Mauritian identity system's storage regime partly because of the lack of judicial oversight for data sharing.[320] The dissenting opinion of the Indian Supreme Court also holds that the government's brazen disregard of the Supreme Court's interim orders to stop the expansion of the Aadhaar project when the constitutional challenge to Aadhaar was being heard signalled a disrespect for the principle of separation of powers rooted in the rule of law and affected the rights of citizens who rely on judicial institutions for the protection of their rights.[321] These courts, by asserting the judiciary's role in securing individual rights within an identity system, suggest that the effective judicial remedies and access to justice for violation of rights are crucial to the framework governing identity systems in countries committed to democracy and the rule of law.

319 *Aadhaar Judgment*, ¶ 353 at 427.

320 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 32–33.

321 *Aadhaar Judgment*, ¶ 337 of dissent.

INCREASED ATTENTION TO THE RIGHTS OF SEXUAL MINORITIES

75. While designing identity systems, it is important to ensure that the rights of trans persons and gender diverse persons are not violated due to a mismatch between their self-identified gender and their sex as recorded in the identity system. The matching of identity is crucial for the realisation of all rights that are dependent on proving identity.

76. The 2018 report[322] of the UN Independent Expert on protection against violence and discrimination discussed the decisions of courts in Botswana, Kenya, Chile, Colombia, Ecuador, India, Pakistan, and Bangladesh, which held that trans persons must be legally recognised, including their right to have their gender identity and, in some cases, their changed name (if any) reflected in identity documents[323]. The report highlights the human rights violations that occur when the names and sex details of individuals in official documents do not match their gender identity or expression. This includes arrest, harassment, abuse, violence and extortion, exclusion from school and the formal labour market, barriers in access to services such as housing, healthcare, and emergency care, and services in times of crisis.[324] Although acknowledging that the manner in which data regarding identity is recorded is crucial to enjoyment of fundamental rights, the Independent Expert questioned the need for the "pervasive exhibition of gender markers in official and non-official documents" and opines that "States must refrain from

322 UN General Assembly, Report of the Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity, A/73/152 (12 July 2018), **https://www.un.org/en/ga/search/view_doc.asp?symbol=A/73/152**

323 UN General Assembly, A/73/152 at 18.

324 UN General Assembly, A/73/152 at 12.

gathering and exhibiting data without a legitimate, proportionate and necessary purpose."[325]

77. Due to the near impossibility of subsequently altering biometric data recorded during the data collection phase of identity systems, it is important to ensure that other data like recorded sex can nevertheless be altered afterwards so that trans persons are not deprived of their basic rights. As the Independent Expert notes, the question of when information on sex is necessary to collect in the first place is also at issue.

325 UN General Assembly, A/73/152 at 12.

INCREASED ENGAGEMENT WITH INTERNATIONAL HUMAN RIGHTS LAW

78. While Mauritius, India, and Jamaica are State Parties to the International Covenant on Civil and Political Rights, and therefore have an obligation to fulfil the rights guaranteed under the Convention, including the right to privacy, the Convention does not find a mention in the judgments analysed on the rights implications of identity systems. The Kenyan High Court briefly mentions the Convention, but little consideration is given to its impact beyond the existence of a right to privacy.[326] The Kenyan High Court's most complete engagement with international human rights law is limited to privacy and data protection principles issued by the OECD and the African Union, which the court cites in evaluating the data protection framework in which the Kenyan national identity system operates.[327]

79. Although the obligations imposed on State Parties to a treaty have important implications for all national authorities, including the executive and the legislature, the judiciary is a key actor in reviewing the compatibility of domestic legislation with international human rights treaties[328] and assessing whether the state is complying with its international obligations. International human rights law also fills gaps at the domestic level through a reliance on international norms and standards. International human rights law can be understood as "part of a broader set of interrelated, mutually reinforcing processes and institutions-interwoven strands in a rope-that together pull human rights forward, and to which international law makes distinctive

326 See *Huduma Namba Judgment*, ¶ 747.

327 See *Huduma Namba Judgment*, ¶¶ 843–846 (comparing the Kenyan data protection framework to established international principles contained in the OECD Privacy Principles and the African Union Convention on Cyber Security and Personal Data Protection).

328 European Commission for Democracy Through Law (Venice Commission), Draft report on the implementation of international human rights treaties in domestic law and the role of courts, **https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL(2014)046-e**

contributions."[329] It is undoubtedly a single strand of the rope, but nevertheless strengthens the entire rope.[330]

80. From the perspective of civil society organisations, international human rights norms and standards can create stronger protection for existing domestic rights and also influence the "development of transformative national-level jurisprudence and law and policy reform."[331] Beyond the legal, introducing the ideas of international human rights law also has an educational effect on society by being a process through which the construction of ideas, identities, and interests of social actors is recast into a more "rights-aligned perspective" – a step forward in the protection of human rights.[332]

329. Douglass Cassel, "Does international human rights law make a difference?," Chicago Journal of International Law 2 (2001): 121.

330 Cassel, "International human rights law," 121.

331 See Johanna B. Fine, Katherine Mayall, and Lilian Sepúlveda, "The role of international human rights norms in the liberalization of abortion laws globally," Health and Human Rights Journal, (2 June 2017), **https://www.hhrjournal.org/2017/06/the-role-of-international-human-rights-norms-in-the-liberalization-of-abortion-laws-globally/ (last visited 20 November 2019)**.

332 Janet E. Lord and Michael Ashley Stein, The Domestic Incorporation of Human Rights Law and the United Nations Convention on the Rights of Persons with Disabilities, (Faculty Publications, 2008), 665.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org