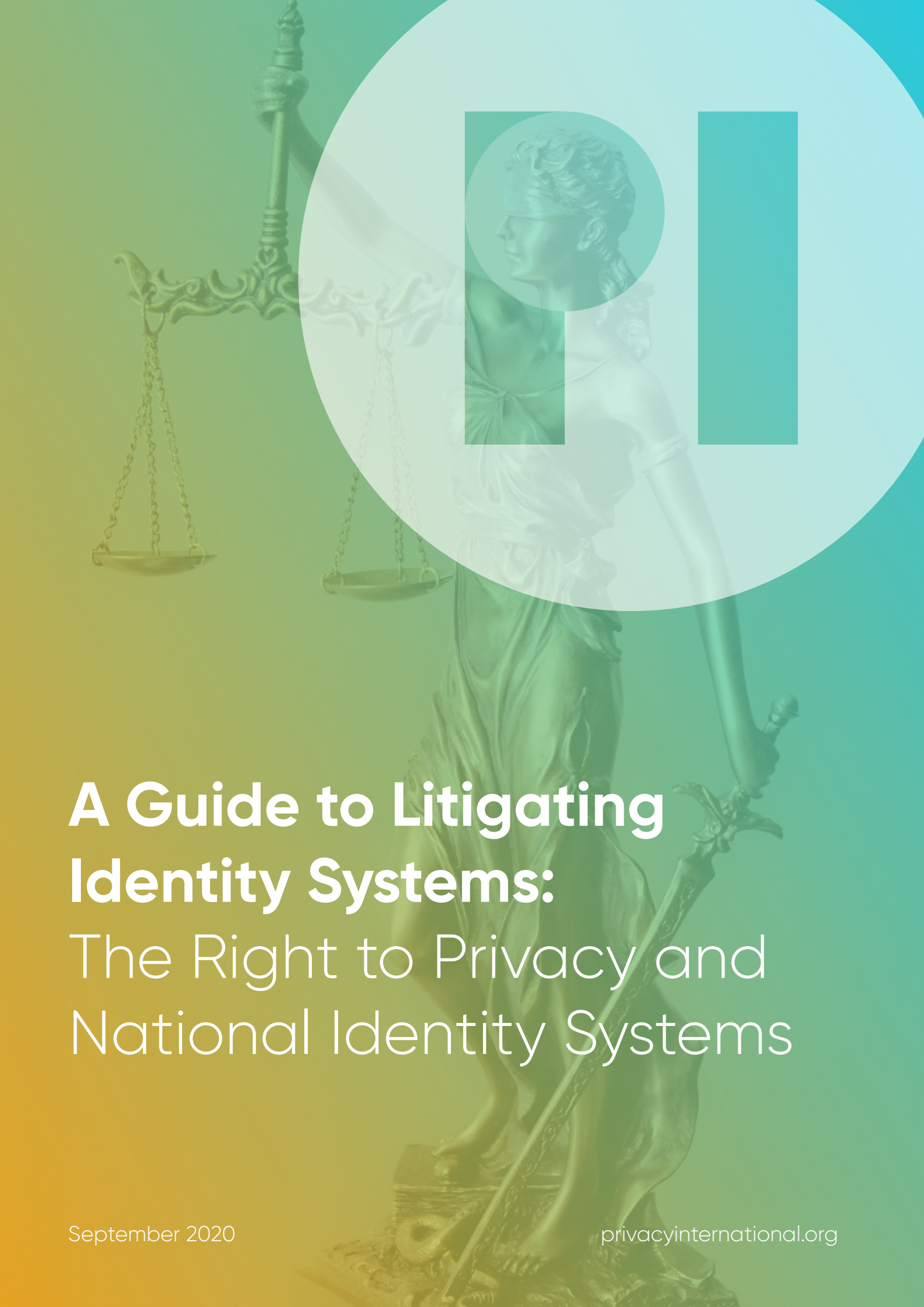

A Guide to Litigating Identity Systems:
The Right to Privacy and National Identity Systems

September 2020

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

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

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

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

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

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

Cover image: Tingey Injury Law Firm

PART 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]

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,

140 *Opinion of Justice Batts*, ¶ 366.

141 *Opinion of Justice Batts*, ¶ 366.

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.

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]

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]

---

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.

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.

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 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]

152 *Aadhaar Judgment*, ¶ 306 of dissent.

153 *Huduma Namba Judgment*, ¶ 922.

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.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org