A Guide to Litigating Identity Systems: An Introduction

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

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).

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

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