Myanmar

Human Rights Analysis of Biometric Digital ID Systems

December 2020

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction[1]

This paper evaluates human rights issues that are relevant for a biometrics-based digital ID system that Myanmar might adopt. Digital ID systems are systems which assign individuals a single "digital ID" which is used to authenticate an individual's identity and generally stored in a central database.[2] They range from so-called soft digital IDs, such as a password used to access a social media account, to more secure sorts of IDs, which are often based on immutable and unique biometric data such as fingerprints or iris scans. While these more secure biometric digital IDs do provide important benefits, such as the inability to crack into them, unlike digital passwords, they also raise a number of complex human rights issues. This is due to issues associated with having a central database of personal data, the potential for abuse of any large-scale data collection exercise and the fact that digital IDs are often used as a mandatory system for accessing certain social services.

This paper comprises four parts. The first part reviews relevant human rights standards. The second presents the legal framework in Myanmar and reviews what we know about current efforts by the government to implement a national digital ID system there. The third part presents a comparative assessment of digital ID systems in India, Kenya and Jamaica, the latter two being countries where courts have found the local digital ID schemes to be unconstitutional. Finally this paper offers recommendations for Myanmar.

1. International Human Rights Standards

Digital ID systems, depending on what information they are based on and how they are used, have the potential to impact a wide range of everyday activities and also human rights. This section of the paper looks at four sets of human rights which are engaged here, namely the right to recognition as a person before the law, the right to equality and non-discrimination, the right to privacy, and social and economic rights.

1.1 The Right to Recognition as a Person Before the Law

Everyone has the right to be recognised everywhere as a person before the law, as guaranteed in Article 6 of the Universal Declaration of Human Rights (UDHR)[3] and Article 16 of the International Covenant on Civil and Political Rights (ICCPR).[4] This right to status as a legal person

---

[1] This Brief was authored by Laura Notess, Legal Officer, CLD, with research support from Hanna Rioseco, Legal Intern, CLD.

[2] See Access Now, National Digital Identity Programmes: What's Next?, May 2018, p. 5. Available at: https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf.

[3] UN General Assembly Resolution 217A (III), 10 December 1948.

[4] UN General Assembly Resolution 2200A (XXI), 16 December 1966, in force 23 March 1976.

is foundational for the realisation of other human rights, because represents an acknowledgement that each person has rights and duties under the law. As noted by the Inter-American Court of Human Rights: "[T]he failure to recognize juridical personality harms human dignity, because it denies absolutely an individual's condition of being a subject of rights and renders him vulnerable to non-observance of his rights by the State or other individuals."[5]

International human rights law also recognises the right of every child to be registered immediately after birth, as well as to have a name and acquire a nationality. This right is protected by Article 7 of the Convention of the Rights of the Child, which Myanmar has ratified, as well as Article 24(2) of the ICCPR. Such registration should be provided to all children without discrimination and regardless of the status of their parents. However, lack of birth registration should not be an obstacle to accessing any key national service.[6] Recognising the importance of birth registration for ensuring the legal recognition of children, Sustainable Development Goal Target 16.9 calls on States to provide "legal identity for all, including birth registration".[7]

In addition to registration of birth, other legal documents, such as ID cards, can serve as proof of legal identity. Practically, in many countries, proof of legal identity is necessary for a range of basic activities, such as accessing social services, voting, obtaining licences, employment and so on. In theory, the ability to exercise one's fundamental human rights, including recognition as a person before the law, should not be conditioned on holding an identity card (absent a compelling reason, justified under international human rights standards). In practice, however, proof of legal identity is often necessary to full realisation of a range of fundamental human rights, including the right to legal personhood. For this reason, government programmes which ensure that individuals can obtain legal ID documents freely may be crucial to the protection of fundamental human rights and can promote practical realisation of the right to recognition as a person before the law.

However, legal ID programmes can also violate human rights or perpetuate inequalities, depending on how they work. If ID documents are not universally available, on a non-discriminatory basis, those who do not have access to them may suffer human rights abuses. Data collection for purposes of providing legal ID documents may raise privacy or surveillance concerns, or perpetuate discrimination depending on the use of sensitive data related to race, ethnicity or religion. Any legal ID programme should therefore carefully consider intersecting human rights issues, which are discussed below.

1.2 Equality and Non-Discrimination

The right to be free of discrimination is protected in several international human rights instruments, including in general terms in the primary human rights treaties and, in reference to particular forms of discrimination, such as based on sex or race, in more specific treaties.[8] For example, Article

[5] Inter-American Court of Human Rights, *The Girls Yean and Bosico v. Dominican Republic*, 8 September 2005, para. 179. Available at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_130_%20ing.pdf.
[6] Human Rights Council, Resolution 28/13 on birth registration and the right of everyone to recognition everywhere as a person before the law, UN Doc. A/HRC/RES/28/13, 7 April 2015. Available at: undocs.org/A/HRC/RES/28/13.
[7] Available at: https://www.un.org/sustainabledevelopment/peace-justice.
[8] See, among others, the Universal Declaration of Human Rights, Article 2(1); International Covenant on Civil and Political Rights, Articles 2(1) and 26; International Convention on the Elimination of All Forms of Racial

2(2) of the International Covenant on Social, Economic and Cultural Rights, which Myanmar has ratified, stipulates that social, economic and cultural rights should be "exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[9]

Discrimination refers to differential treatment, based on a specific prohibited ground, such as race or religion, which impairs the recognition, exercise or enjoyment of human rights or social benefits or entitlements, such as a job. Differential treatment will be considered to be discriminatory unless it can be justified as being reasonable and objective.[10] To be considered reasonable and objective, the differential treatment must have a legitimate basis that is compatible with human rights standards and has the sole purpose of promoting the general welfare in a democratic society. The effect of the differential treatment must also be proportionate in the sense that the benefits flowing from are greater than the harm it causes to equality.[11]

States are obliged to take measures to eliminate both direct and indirect or systemic discrimination. Direct discrimination "occurs when an individual is treated less favourably than another person in a similar situation based on a prohibited ground."[12] Indirect discrimination, on the other hand, refers to laws or implementation which appear to be neutral in nature but which differentially impact certain groups identified by reference to a protected ground.[13]

In the context of legal ID systems, direct discrimination may arise if ID documents are denied to certain persons based on a protected ground, either under the law or through implementation. Indirect discrimination would arise if the ID system disproportionately fails to work in practice for certain groups due to characteristics relating to their group membership. Digital ID systems, for example, may indirectly discriminate against the poor, who typically have less digital literacy and access to technology.[14] In this case, where digital IDs become widely used as a means of verification for accessing social services, financial services, voting or other basic services, a lack of access to them can have a cascading discriminatory impact.

Difficult and challenging questions are raised by ID systems which contain information about race, religion, ethnicity or other protected grounds, which may then serve as a basis for discrimination. Including such information can facilitate discrimination by making such groups easy to identify,

---

Discrimination, General Assembly Resolution 2106 (XX), 21 December 1965, in force 4 January 1969; Convention on the Elimination of All Forms of Discrimination against Women, General Assembly Resolution 34/180, 18 December 1979, in force 3 September 1981; and Convention on the Rights of Persons with Disabilities, General Assembly Resolution 61/106, 13 December 2006, in force 3 May 2008.

[9] UN General Assembly Resolution 2200A (XXI), 16 December 1966, in force 3 January 1976.

[10] Committee on Economic, Social and Cultural Rights, General Comment 20, 2 July 2009, U.N. Doc. E/C.12/GC/20, para. 13. Available at: https://www.refworld.org/docid/4a60961f2.html. The same "reasonable and objective" language is also used in deciding whether differential treatment is permissible under the non-discrimination provisions of the ICCPR. See Human Rights Committee, General Comment No. 18, 10 November 1989, para. 13. Available at: https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/INT_CCPR_GEC_6622_E.doc.

[11] General Comment 20, *ibid.*, para. 13.

[12] General Comment 20, *ibid.*, para. 10(a).

[13] General Comment 20, *ibid.*, para .10(b).

[14] Special Rapporteur on Extreme Poverty and Human Rights, Report submitted in accordance with Human Rights Council Resolution 35/19, 11 October 2019, para. 45. Available at: https://undocs.org/A/74/493.

thereby enabling differential treatment. In very serious cases, such ID systems can facilitate grave human rights abuses. The Committee on the Elimination of Racial Discrimination lists "[c]ompulsory identification against the will of members of particular groups, including the use of identity cards indicating ethnicity" as a potential indicator for the presence of genocide.[15]

Overall, given the serious risk of discrimination, a number of human rights bodies and experts have advised against including protected grounds as identifiers in ID systems.[16] At a minimum, where such identifiers serve to enable enforcement of discriminatory laws or operate in a context where there is strong systemic discrimination, their inclusion in ID systems may well result in discrimination in practice. In such instances, these identifiers should not be included in ID systems.

If identifiers such as ethnicity or religion are included in ID systems, individuals should have freedom to self-select these characteristics. In addition, the options under them should not be limited to a closed list which excludes certain groups since this may constitute discrimination against groups which are not listed through failing to acknowledge their existence. For example, various UN experts opposed Iran's removal of an "other" religion category on ID documents, which left only four officially recognised religions.[17] Similarly, the UN Special Rapporteur on Freedom of Religion and Belief has noted that even if including religion in an identity system was acceptable, limiting the choice to three religions was discriminatory and a violation of international law.[18] Better practice suggests that such identifiers should not be included at all, but if they are included, self-identification should applied.

1.3 Privacy

The right to privacy is guaranteed by Article 12 of the UDHR and Article 17 of the ICCPR. According to the latter, the right to privacy includes the right to be free from arbitrary or unlawful interference with one's privacy, family, home or correspondence. It is based on the idea that individuals should enjoy a "private sphere" of autonomous development and interaction that is free

[15] Committee on the Elimination of Racial Discrimination, Decision to Follow-Up to the Declaration on the Prevention of Genocide: Indicators of Patterns of Systematic and Massive Racial Discrimination, 14 October 2005, U.N. Doc. CERD/C/67/1. Available at: https://www.ohchr.org/Documents/HRBodies/CERD/indicators_for_genocide.doc.

[16] Committee on the Elimination of Racial Discrimination, Concluding Observations of the Committee on the Elimination of Racial Discrimination: Indonesia, 15 August 2007, para. 21 (recommending that Indonesia remove religion as a category), available at: https://www.ecoi.net/en/file/local/1079411/470_1219158150_cerd-c-idn-co-3.pdf; European Court of Human Rights, *Sinan Işık v.Turkey*, Application No. 21924/05, 2 February 2010 (finding that a mandatory religion field was a violation of freedom of religion), available at: http://hudoc.echr.coe.int/tur?i=001-97087; and Abdelfattah Amor, Special Rapporteur on the question of religious intolerance, Visit by the Special Rapporteur to Pakistan, 2 January 1996, U.N. Doc. E/CN.4/1996/95/Add.1, paras. 23-24, 45 and 85, available at: https://undocs.org/E/CN.4/1996/95/Add.1.

[17] Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Special Rapporteur on minority issues and Special Rapporteur on freedom of religion or belief, Letter to the Government of Iran, 17 February 2020. Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25069.

[18] Special Rapporteur on freedom of religion or belief, Report to the Commission on Human Rights, 16 January 2004, UN Doc. E/CN.4/2004/63, para. 42. Available at: https://undocs.org/E/CN.4/2004/63.

from excessive unsolicited and uninvited intrusions from other people.[19] The right to privacy is broad and covers, among other things, communications and any information that "may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication."[20]

Article 17 requires any interference with the right to privacy to be both lawful and not arbitrary. This means that restrictions on this right, including rules about the collection of data, should be clearly authorised by law. Furthermore, to ensure that restrictions are not arbitrary, international standards suggest that any interference should be in accordance with the objectives of the ICCPR and be "reasonable in the particular circumstances". The former implies that any interference should be proportionate in the sense that the harm to privacy is outweighed by the benefits that flow from the interference and that if a less intrusive option for securing the benefits is available, that option should be used.[21]

The right to privacy requires States to regulate by law the gathering and holding of personal information (data protection). This includes rules to ensure that personal information is not accessed by individuals who do not have a legal right to access it and is not used in a manner which is incompatible with human rights. Individuals should have the ability to confirm which bodies, whether public or private, hold their personal information, to correct inaccurate information and to have information that was gathered unlawfully deleted.[22]

Biometric data is extremely sensitive because it is inseparably linked to a particular person and cannot be changed. The UN High Commissioner for Human Rights has noted that biometric data has the potential to be gravely abused and that there is a particular risk where large amounts are stored in a single, centralised database.[23] Identity theft involving biometric data, for example, is extremely difficult to remedy. In addition, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals.[24]

Given these risks, the European Union's General Data Protection Regulation identifies biometric data (along with other data, such as data about racial or ethnic origin or religious beliefs), as "special category" data which should not normally be processed, subject only to narrowly defined exceptions.[25] The Human Rights Committee has also indicated that a requirement to provide fingerprints or retinal scans to obtain social assistance is a breach of the right to privacy.[26]

[19] Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, 3 August 2018, para. 11. Available at: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/39/29.
[20] *Ibid.*, para. 6.
[21] Human Rights Committee, General Comment No. 16, 8 April 1988, paras. 3-4. Available at: https://www.refworld.org/docid/453883f922.html.
[22] *Ibid.*, para. 10.
[23] Report of the UN High Commissioner for Human Rights, note 19, para. 14.
[24] *Ibid*.
[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 9. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[26] Human Rights Committee, Concluding Observations of the Human Rights Committee, 7 April 1999, U.N. Doc. CCPR/C/79/Add.105, para. 16. Available at: https://undocs.org/CCPR/C/79/Add.105.

Given the risks, data intensive systems (especially those that collect and store biometric data) should only be deployed "when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim."[27] Furthermore, independent oversight of such systems is absolutely crucial. States should establish or maintain "independent, effective domestic oversight mechanisms capable of ensuring . . . accountability for State surveillance of communications, their interception and the collection of personal data".[28]

Finally, digital ID systems that are linked to any kind of surveillance system raise additional human rights concerns regarding privacy and possibly other civil and political rights, such as the right to freedom of expression. Laws governing surveillance regimes should ensure that they:

(a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;
(b) Are strictly and demonstrably necessary to achieve a legitimate aim; and
(c) Adhere to the principle of proportionality and are not employed when less invasive techniques are available or have not yet been exhausted.[29]

Any actual surveillance should be based on an individual justification and be subject to a proportionality analysis, which cannot occur when mass surveillance is undertaken.[30] Surveillance regimes which require the collection and indefinite retention of personal data are simply not proportionate. [31] In 2016, in Concluding Observations regarding Kuwait, the Human Rights Committee addressed the privacy impacts of a Kuwaiti counter-terrorism law which enabled DNA testing and the creation of a centralised database on DNA. Their concerns, which highlight the possible pitfalls for any surveillance regime which relies on the collection of sensitive biometric data, included: the compulsory nature and sweeping scope of DNA testing; the broad powers of authorities to collect DNA samples; the lack of clarity on safeguards to ensure confidentiality and prevent arbitrary use of the DNA samples; and the absence of independent oversight.[32] As a result, any surveillance system which relies on biometric data should have transparent, clearly defined rules and oversight, along with strong safeguards and limits on the ability of authorities to access and use the data.

1.4 Social and Economic Rights

Legislation that requires the use of a digital ID for access to goods and services might limit the ability of persons who do not qualify for or otherwise cannot obtain a digital ID to access those services. Where access to public benefits is limited, this may constitute a restriction on the right to health, education, food, employment or other social and economic rights. More generally, inasmuch as a digital ID programme is integrated into a system for distributing welfare

[27] Report of the UN High Commissioner for Human Rights, note 19, para. 61(c).
[28] UN General Assembly Resolution 68/167, 18 December 2013, paras. 4(c)-(d). Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.
[29] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, para. 83. Available at: https://undocs.org/A/HRC/23/40.
[30] Report of the UN High Commissioner for Human Rights, note 19, para. 17.
[31] *Ibid.*, para 18.
[32] Human Rights Committee, Concluding Observations on the Third Periodic Report of Kuwait, 11 August 2016, U.N. Doc. CCPR/C/KWT/CO, para. 20. Available at: https://undocs.org/en/CCPR/C/KWT/CO/3.

entitlements, this may not serve the best interests of the poorest and most vulnerable. The UN Special Rapporteur on Extreme Poverty and Human Rights has commented extensively on the potential risks of a digital welfare system:

> First, the process for determining eligibility may easily be transformed into an electronic question-and-answer process that almost inevitably puts already vulnerable individuals at even greater disadvantage.
>
> Second, the way in which determinations are framed and communicated may be dehumanized and allow no room for meaningful questioning or clarification.
>
> Third, the digital welfare state often seems to involve various forms of rigidity and the robotic application of rules. As a result, extenuating circumstances . . . are often not taken into account in a predominantly digital context.
>
> Fourth, digital systems are often not designed to respond rapidly either to serious emergencies or to daily challenges, such as those that may be experienced by an older person whose entitlement has suddenly and inexplicably been electronically reduced or cancelled or by a single parent unable to take a child to a local day care because the digital identification card will not function.
>
> Fifth, the ways in which services are provided can easily have degrading connotations, such as unnecessarily exposure to a broader audience the fact that a person is reliant on benefits, or requiring extended waiting periods or the navigation of lengthy queues.
>
> Sixth, the introduction of various new technologies that eliminate the human provider can enhance efficiency and provide other advantages but might not necessarily be satisfactory for individuals who are in situations of particular vulnerability. New technologies often operate on the law of averages, in the interests of majorities and on the basis of predicted outcomes or likelihoods.[33]

2. *Digital ID Developments in Myanmar*

2.1 Legal Framework

Article 357 of Myanmar's Constitution provides for the protection of "privacy and security of home, property, correspondence and other communications of citizens under the law", subject to other constitutional provisions.[34] Myanmar's 2017 Law Protecting the Privacy and Security of Citizens also sets out protections for the privacy and security of communications.[35] Specifically, in addition to affirming the constitutional right to privacy, it places a general obligation on authorities to protect privacy (Article 4) and prohibits them from entering private residences, conducting surveillance, intercepting communications, obtaining telephonic or electronic communications and other similar activities without prior authorisation (Article 8).

[33] Special Rapporteur on Extreme Poverty and Human Rights, note 14, paras. 54-59.
[34] English translation available at: https://www.constituteproject.org/constitution/Myanmar_2008.pdf?lang=en.
[35] Law Protecting the Privacy and Security of Citizens, 8 March 2017. Available in English at: https://www.myanmar-responsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf.

However, there are important limits to the way the 2017 Privacy Law protects privacy. First, Article 2(c) defines privacy is a very limited and odd way to include the rights to freedom of movement, freedom of residence and freedom of speech of a citizen, in accordance with the law. While these rights are important, they are different from privacy, which this definition simply does not cover. In particular, and notably for our purposes, this definition does not include a right to privacy in relation to personal information, such as one's biometrics or other identifying information. It is unclear how far other provisions in the Law remedy this problem.

Second, the protections in the Privacy Law are by design weak. All that is required to overcome the Article 8 protections, including against surveillance and search and seizure, is "permission from the Union President or a Union-level Government body" (or a lawful order, permission or warrant). Thus, any Union-level public authority can essentially authorise itself to avoid these protections. Better practice is to require court authorisation for actions like surveillance and search and seizure.

Third, there is no system of oversight for these protections, apart from the right to appeal to the courts, which is not something most Myanmar citizens can afford to do. International standards call for an accessible and independent administrative system of oversight for at least data protection regimes.

Fourth, due to amendments in August 2020, the scope of the Privacy Law was limited to "competent authorities", essentially government actors. This means that this Law does not provide any protection at all against breaches of privacy committed by private actors.

Fifth, at least some of the protections are unclear. For example, the prohibition on surveillance is conditioned on the surveillance disturbing "their privacy and security or affect their dignity". It is not clear what would trigger this. In any cases, most countries prohibit all official surveillance unless it can be justified, for example based on the need to investigate a crime.

Myanmar also does not have any specific data protection rules. The 2017 Privacy Law does not establish any general rules around the collection and management of personal data, including biometric data, by government or private actors. All it does is prohibit officials from demanding or obtaining personal telephonic or electronic communications data from telecommunication operators without an authorisation, which is clearly not the same thing at all. The 2013 Telecommunications Law also does not provide for personal data protection, although it does prohibit unauthorised actors from accessing secure data without a court order.[36]

Ultimately, Myanmar lacks strong privacy protection or a regime governing personal data. This is a major legal gap which should be filled before any digital ID regime is established.

2.2 Background: Identification Cards in Myanmar

[36] Telecommunication Law No. 31 of Myanmar, 8 October 2015, Articles 69, 75-7. Available in English at: http://www.asianlii.org/mm/legis/laws/tlhln312013511/.

The primary ID cards in Myanmar are "Citizenship Scrutiny Cards" (CSC). These are issued under the 1982 Citizenship Law and its accompanying 1983 Procedures. The CSCs replaced National Registration Cards, which were issued under the 1949 Residents of Myanmar Registration Act, although many residents of Myanmar still have National Registration Cards as their primary form of identification and, in colloquial use, the terms are sometimes used interchangeably. CSCs include, among other information, the individual's race and religion.[37] Anyone who does not have a CSC may not be able to undertake certain basic activities, including to vote,[38] travel within Myanmar, buy property, obtain a passport,[39] or graduate/obtain a diploma.[40]

There are three primary types of CSCs: those for full citizens (colour-coded pink), those for associate citizens (blue) and those for naturalised citizens (green). This tiered citizenship approach is based in the 1982 Citizenship Law. Full citizens are "nationals such as the Kachin, Kayah, Karen, Chin, Burman, Mon, Rakhine or Shan and ethnic groups as have settled in any of the territories included within the State as their permanent home from a period anterior" to 1823, when British occupation began in Arakan State.[41] The President or the Union Government (formerly the Council of State) has the power to decide whether an ethnic group is a national one the members of which fall into this category.[42] It is also possible to gain full citizenship in some other ways, based on various combinations of the citizenship status of one's parents.[43]

Persons lacking membership in the necessary ethnic groups or proof of the appropriate parental status may be able to obtain associate or naturalised citizenship. These forms of citizenship may be revoked more easily than full citizenship and, while associate and naturalised citizens generally enjoy the same rights as full citizens, these rights may be limited at the discretion of the president or the Union government.[44] Associate citizenship is granted to those who qualified and applied for

[37] Procedures as described in Justice Base, A Legal Guide to Citizenship and Legal Identity Document in Myanmar, December 2018. Available at: http://justicebase.org/wp-content/uploads/2020/09/12.2018-Legal-Guide-to-Citizenship-Documentation_ENG_FINAL-1.pdf.

[38] Jose Maria Arraiza and Olivier Vonk, Report on Citizenship Law: Myanmar, October 2017, p. 9, available at: https://cadmus.eui.eu/bitstream/handle/1814/48284/RSCAS_GLOBALCIT_CR_2017_14.pdf; and Myanmar News Agency, Issuing Citizenship Scrutiny Cards Speeded Up to Ensure Voting Right, 3 August 2020, Global New Light of Myanmar, available at: https://www.gnlm.com.mm/issuing-citizenship-scrutiny-cards-speeded-up-to-ensure-voting-right/.

[39] Center for International Human Rights at Northwestern Pritzker School of Law, Myanmar: 3rd UPR Cycle, 7 July 2020, available at: https://www.law.northwestern.edu/legalclinic/humanrights/documents/final-myanmar-report.pdf; and Julia Wallace, Myanmar Casts Minorities to the Margins as Citizenship law Denies Legal Identity, 3 November 2016, available at: https://www.theguardian.com/global-development/2016/nov/03/myanmar-casts-minorities-to-margins-citizenship-law-denies-legal-identity.

[40] Australian Department of Foreign Affairs and Trade, DFAT Country Information Report: Myanmar, 18 April 2019, para. 3.31, available at: https://www.dfat.gov.au/sites/default/files/country-information-report-myanmar.pdf; and Human Rights Council, Report of the Special Rapporteur on the Situation of Human Rights in Myanmar, 23 March 2015, available at: https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session28/documents/a_hrc_28_72_en.doc.

[41] Citizenship Law, 15 October 1982, section 3. Available at: https://www.refworld.org/docid/3ae6b4f71b.html.

[42] *Ibid.*, s. 4. The term "Council of State" in the original law is now interpreted by the 2011 Law Relating to the Adaption of Expressions. For an explanation of the history of this change, see International Commission of Jurists, Citizenship and Human Rights in Myanmar: Why Law Reform is Urgent and Possible, June 2019. Available at: https://www.icj.org/wp-content/uploads/2019/06/Myanmar-Citizenship-law-reform-Advocacy-Analysis-Brief-2019-ENG.pdf.

[43] Citizenship Law, note 41, sections 5-7.

[44] *Ibid.*, sections 30(c), 35, 53(c) and 58.

citizenship under the (now repealed) 1948 citizenship law.[45] People may seek naturalised citizenship if they can provide "conclusive evidence" that they entered and resided in Myanmar prior to independence in 1948[46] or whose parents hold certain specified combinations of citizenship status (unlike the categories for full citizenship, these are based on only one parent having some sort of citizenship status). Applicants must also be eighteen years old, be able to speak one of the national languages and be of good character and sound mind.[47]

This three-tiered citizenship structure introduces complexities into the process of issuing identity cards. Members of ethnic minority groups that are not on the list of the 135 ethnic groups which are eligible for full citizenship face greater difficulties in obtaining CSCs.[48] They may face challenges in meeting the evidentiary and other requirements necessary to show associate or naturalised citizenship. The government has tried alternative approaches to issuing ID cards to them. For example, during the 1990s, the government issues a large number of Temporary Registration Cards. These were originally intended as temporary cards for those who had pending applications for National Registration Cards. However, these Temporary Registration Cards were distributed widely to residents of Rakhine State who could not obtain CSCs and effectively took the place of official ID cards for many years.[49]

In 2015, the government withdrew the Temporary Registration Cards, required people holding them to surrender them and replaced them with temporary registration "receipts".[50] It then introduced National Verification Cards as a replacement. According to the President Office, the National Verification Cards were intended as a step towards examining whether a person was entitled to become a citizen in accordance with the 1983 Citizenship Law and to acknowledge such persons as Myanmar residents.[51]

In practice, this process has been controversial, partly because the National Verification Cards do not confer full citizenship rights and some observers believe they are a means of identifying and targeting members of the Rohingya community. The UN High Commissioner for Human Rights, for example, has criticised the National Verification Card as a "document which denies [the Rohingya] citizenship, leaving them stateless and restricting their access to basic services or free movement."[52] Many Rohingya also oppose the National Verification Cards and are unwilling to obtain one. However, some reports indicate that obtaining a card has effectively been made mandatory, by requiring possession of a card in order to participate in local elections or to obtain

[45] *Ibid.*, chapter 3.
[46] *Ibid.*, chapter 4.
[47] *Ibid.*, section 44(b-e).
[48] Julia Wallace, note 39.
[49] Arraiza and Vonk, note 38, p. 9.
[50] SMILE Myanmar, The Seagull: Human Rights, Peace and Development, Free Rohingya Coalition (FRC), Burmese Rohingya Organisation UK (BROUK), the International State Crime Initiative (ISCI) and The Institute on Statelessness and Inclusion (ISI), Joint Submission to the Human Rights Council, Universal Periodic Review, 9 July 2020 (citing Presidential Notification 15/2015). Available at: https://files.institutesi.org/UPR37_Myanmar.pdf.
[51] President Office, Republic of the Union of Myanmar, Identity Card for National Verification in Rakhine to Return. Available at: https://www.president-office.gov.mm/en/?q=issues/rakhine-state-affairs/id-7031.
[52] Michelle Bachelet, UN High Commissioner for Human Rights, Oral Update on the Human Rights Situation of Rohingya People, 30 June 2020. Available at: https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=26018&LangID=E.

fishing and boating licences, among other things.[53] There have also been allegations of abuse by security forces linked to registration efforts for National Verification Cards.[54]

In summary, national ID cards in Myanmar are necessary for engaging in a number of basic activities. Because issuing national ID cards is based on a tiered approach to citizenship and due to challenges around non-recognition of the Rohingya and other minority groups as citizens, any attempt to convert the system to a digital one is likely to be contentious.

2.3 Digital ID Proposals

In recent years, Myanmar's Ministry of Labour, Immigration and Population has announced plans to replace paper citizenship cards with "smart cards" as a part of a digital ID regime that would use biometric data. However, no legal framework yet exists for this and, to our knowledge, there is also no policy document for it.

The idea of a digital ID regime was under consideration at least as far back as 2013, although plans for furthering the project were apparently delayed due to lack of funding.[55] In 2016, both Myanmar's 12-point Economic Policy and its e-Governance Master Plan for 2016-2020 indicated that the creation of a digital ID card was a priority.[56] In 2017, the Ministry of Labour, Immigration and Population announced pilot projects in select regions to replace traditional ID cards with digital versions.[57] Following the pilot, the intent was to develop a national plan for digital ID cards for all citizens over the age of 18.[58]

News reports from 2020 now indicate that the intention is to roll out the digital ID system over two years, in three phases.[59] This has the support of an agreement between Myanmar and Austria on a loan to fund the project, although it is not clear how COVID-19 may affect the planned timeline. While the government has hosted some workshops and discussions on the digital ID regime, no broad-based consultation on it has taken place so far. There seems to be some recognition of a need for greater consultation among officials, In May 2020, Tatmadaw MP Major

[53] Report of the Special Rapporteur on the Situation of Human Rights in Myanmar, 20 August 2018, U.N. Doc. A/73/332, para. 62. Available at: https://undocs.org/A/73/332.
[54] *Ibid.*, para. 62; and Shoon Naing, Myanmar Forces Rohingya to Accept Cads that Preclude Citizenship: Group, 3 September 2019, Reuters, available at: https://www.reuters.com/article/us-myanmar-rohingya-idUSKCN1VO16D.
[55] Privacy International, The Right to Privacy in Myanmar, March 2015. Available at: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=2122&file=EnglishTranslation.
[56] Government of Myanmar, Myanmar e-Governance Master Plan 2016-2020, available at: https://www.motc.gov.mm/sites/default/files/Myanmar%20e-Governance%20Master%20Plan%20%282016-2020%29%20English%20Version%28Draft%29.pdf; and Economic Policy of the Union of Myanmar, 2016, available at: https://themimu.info/sites/themimu.info/files/documents/Statement_Economic_Policy_Aug2016.pdf.
[57] Aung Kyaw Min, 'Smart' ID Pilot Project Rolls Out in 4 Test Areas, 13 January 2017, Myanmar Times. Available at: https://www.mmtimes.com/national-news/24538-smart-id-pilot-project-rolls-out-in-4-test-areas.html.
[58] GovInsider, Myanmar Launches Digital Identities for Citizens, 11 January 2017. Available at: https://govinsider.asia/innovation/myanmar-launches-digital-identities-for-citizens.
[59] Chan Mya Htwe, Myanmar to Receive Austrian Loan for National e-ID System, 28 May 2020, available at: https://www.mmtimes.com/news/myanmar-receive-austrian-loan-national-e-id-system.html; and Ministry of Information, Republic of Myanmar, E-IDs Fundamental to E-governance: U Thein Swe, 23 January 2020, available at: https://www.moi.gov.mm/moi:eng/news/362.

Saw Kyaw Aung was quoted as saying that Myanmar should consider the experiences of other countries with digital ID regimes and consult with local and international experts.[60]

No detailed information on the scope of the project has been made publicly available so far. However, the new digital ID system would reportedly collect individuals' biometric data, assign them a unique identity (UID) number and register their data in a database.[61] It is also not clear what biometric data would be used. The 2017 pilot reportedly involved fingerprints, photographs and iris scans.[62] A July 2020 news report suggests that the smartcard would include "personal information of the holder such as photograph, address, employment, blood type, and finger print."[63]

The project appears to have several international backers. The 2017 pilot was reportedly supported by the World Bank, the International Organisation for Migration and some private companies.[64] Austria is providing an interest-free loan to support the development of the digital ID system,[65] while Austrian company OeSD will be involved in project implementation.[66] French multinational company Thales Group is also supporting the project.[67]

It appears that some data collection for the digital ID database has already begun. In May 2019, the Minister of Labour, Immigration and Population said that the agency had already digitised the information of some 1.3 million citizens. According to a news release, this data has been gathered from telecom operators, Myanmar passport offices, offices issuing overseas labour certificates and the Certificates of Identification issued to migrant workers in Thailand. [68]

2.4 Biometric Data Collection

Despite not having in place a strong legal framework for this, there appear to be some initiatives underway already to collect biometric data. The most notable of these is biometric data collection linked to mandatory SIMs card registration. Since 2017, Myanmar has required phone operators to register buyers of each SIM card sold, including the subscriber's name, citizenship ID, birth

[60] Chan Mya Htwe, *ibid*.
[61] E-IDs Fundamental to E-Governance, note 59.
[62] Aung Kyaw Min, note 57.
[63] Myanmar Business Today, Myanmar Working on e-ID for its e-Government Goal, 27 July 2020. Available at: https://mmbiztoday.com/myanmar-working-on-e-id-for-its-e-government-goal.
[64] Aung Kyaw Min, note 57.
[65] Sit Htet Aung, Austria Agrees to Fund Electronic National ID, 23 October 2019, available at: https://www.mmtimes.com/news/austria-agrees-fund-electronic-national-id.html; and Myanmar News Agency, E-IDs Fundamental to E-Governance: U Thein Swe, 23 January 2020, available at: https://www.gnlm.com.mm/e-ids-fundamental-to-e-governance-u-thein-swe.
[66] Myanmar News Agency, E-ID System Working Committee Discusses Finishing Touches to Contract with Austrian Company, 2 November 2019. Available at: https://www.gnlm.com.mm/e-id-system-working-committee-discusses-finishing-touches-to-contract-with-austrian-company.
[67] Myanmar International Television, E-ED/E-Passport: Workshop Jointly Organised with MOLIP and Thales, 22 January 2020. Available at: https://www.myanmaritv.com/news/e-ide-passport-workshop-jointly-organized-molip-and-thales.
[68] Myanmar Times, Government Begins Digitizing Personal Information for ID cards, 9 May 2019. Available at: https://www.mmtimes.com/news/govt-begins-digitising-personal-information-id-cards.html.

date, address, nationality and gender.[69] According to a June 2020 news report, new rules will now require users to have their fingerprints scanned when they register for SIM cards; facial photos will also be stored for "biographic information".[70]

The information collected is stored in a biometric database. The Posts and Telecommunications Department (PTD) of the Ministry of Transport and Communications (MOTC) is reportedly drawing upon the Universal Service Fund to provide financing for the SIM card biometric database.[71] The PTD's tender for bids to provide biometric data storage closed on 9 June 2020.[72] The PTD said that the database, which must be capable of storing up to 60 million biometric records, would be implemented six months after a contract with the winning bidder had been signed.[73]

Other than the SIM card database, biometric data has reportedly been collected as part of the National Verification Card issuance program since October 2017.[74]

3. Comparative Case Studies

3.1 India

India's digital ID regime, known as 'Aadhaar', assigns a 12-digit ID number to each resident of India. It does not have any link to citizenship or immigration status and is instead based solely on residence (specifically having lived in India for at least 182 days during the past one year).[75] The ID number is linked to biometric data (fingerprints and iris scans and, more recently, facial images) as well as other data (name, address and date of birth but not race or religion).[76] Verifying a person's identity then requires both the Aadhaar number and another means of verification, such as a fingerprint, iris scan or a one-time password sent to the user's mobile phone and these need to match when compared to the stored data to verify identity.[77] Aadhaar is used not only by the

[69] Myanmar Times, SIM Card Registration to be Enforced in 2017, 3 August 2016. Available at: https://www.mmtimes.com/business/technology/21728-sim-card-registration-to-be-enforced-in-2017.html.
[70] Myanmar Times, Myanmar Diverts Special Telecoms Fund Biometrics Database, 11 June 2020. Available at: https://www.mmtimes.com/news/myanmar-diverts-special-telecoms-fund-biometrics-database.html.
[71] *Ibid*.
[72] Myanmar Times, Myanmar Wants Mobile User Biometrics, 5 December 2019. Available at: https://www.mmtimes.com/news/myanmar-wants-mobile-user-biometrics.html.
[73] Myanmar Times, Myanmar Diverts Special Telecoms Fund Biometrics Database, note 70.
[74] Australian Department of Foreign Affairs and Trade, note 40. See also President Office, Republic of the Union of Myanmar, National Verification Cards in Maungtaw. Available at: https://www.president-office.gov.mm/en/?q=issues/rakhine-state-affairs/id-8047.
[75] Aadhaar Act, Section 2(v) and 9. Available at: https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.
[76] Privacy International, Initial Analysis of Indian Supreme Court decision on Aadhaar, 26 September 2018. Available at: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar.
[77] Aria Thaker, Aadhaar's Most Common Use is also One of its Most Dangerous Problems, 25 September 2018, Quartz India. Available at: https://qz.com/india/1399518/whatever-indias-supreme-court-says-aadhaar-was-never-a-photo-id/.

government to verify a person's identity but also by private actors, for example to authenticate the identity of an employee or a customer.[78] The entire project is overseen by the Unique Identification Authority of India (UIDAI).

India began implementation of Aadhaar in 2010. As enrolment reached one billion in 2016, the system received a firm basis in law with the passage of the Aadhaar Act.[79] The fact that the project did not have a clear legal basis until 2016 was a major concern, resulting in serious questions over a lack of legal protections around the use of the collected biometric data, a number of legal challenges and confusion over aspects of its implementation.[80] In addition, after the adoption of the 2016 Act, it was subject to a constitutional challenge. In 2017, the Supreme Court, in a landmark ruling, affirmed that the right to privacy was constitutionally protected in India.[81] Then, in 2018, in a judgment addressing Aadhaar more particularly, the Court found that the Aadhaar Act in general was constitutional but placed a number of limits on its scope and application, discussed further below.[82]

Aadhaar has had some notable successes. Its use is now widespread – one estimate says 95% of adults have Aadhaar and use it once a month – and, for some of the poorest residents in India, it is the only form of ID that they have.[83] Some research indicates that Aadhaar has facilitated access to services for more people. For example, the proportion of women who have bank accounts has grown substantially. Government officials also argue that the programme has allowed them to promote better targeting so that government services, such as food subsidies, healthcare and pensions, reach the intended beneficiaries.[84]

On the other hand, the programme has been controversial. Some of the concerns raised can serve as key lessons for any similar system in Myanmar.

Privacy

India's Supreme Court recognised the right to privacy in 2017 and called on the government to enact stronger data protection rules. However, in its 2018 judgment, it still found that that the Aadhaar Act was constitutional. The majority held that the Act, overall, did not violate the right to privacy, finding that the purpose of the Act, namely to ensure that government benefits "actually

[78] Sushil Kambampati, Aadhaar: the Indian Biometric ID System has Potential but Presents Many Concerns, 14 February 2018, Heinrich Boll Stiftung. Available at: https://www.boell.de/en/2018/02/07/aadhaar-indian-biometric-id-system-has-potential-presents-many-concerns.
[79] Privacy International, note 76.
[80] Sushil Kambampati, note 78; and Privacy International, Biometrics: Friend of Foe of Privacy, 2017, p. 10, available at: https://www.privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf.
[81] *Puttaswamy v. India*, 2017. Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.
[82] *Puttaswamy v. India*, 2018. Available at: https://scobserver-production.s3.amazonaws.com/uploads/case_document/document_upload/457/Aadhaar_35071_2012_FullJudgement-1-567.pdf.
[83] Sushil Kambampati, note 78; and State of Aadhaar, Top 10 Insights. Available at: https://stateofaadhaar.in/top-10-insights.php.
[84] OECD, Case Study: Aadhaar – India, 2018. Available at: https://www.oecd.org/gov/innovative-government/India-case-study-UAE-report-2018.pdf.

reach the populace for whom they are meant", was a legitimate aim.[85] However, the Court still placed important limits on the Act out of concern for privacy.

In particular, the Court decided that a provision permitting government entities and private actors to use an Aadhaar number to establish someone's identity for "any purpose" was not valid, holding that it provided too much scope to invade user privacy. It also struck down a rule linking Aadhaar with SIM card registration and bank accounts.

Based in part on the Court's decision in the 2017 case, as well as public concern about the privacy impacts of Aadhaar, a Data Protection Bill is under currently consideration in India's Parliament.[86]

Mandatory Nature and Impacts on Vulnerable Groups

Aadhaar was initially meant to be voluntary but the scope of the project increased with the Aadhaar Act of 2016 and subsequent licensing agreements making enrolment effectively mandatory to access a wide range of services, such as government funding, pensions, banking, insurance and telecommunications.[87] This led to denial of services to persons without an Aadhaar number or who experienced technical issues with the system. For example, impoverished families were denied food rations because they did not have an Aadhaar number, it had not been properly linked to their food ration card or their biometrics authentication failed. Elsewhere, children without Aadhaar numbers lost access to free meals, enrolment in government schools or scholarships.[88]

In its 2018 Supreme Court judgment, the Court imposed limits on the use of Aadhaar, finding that it could only be made mandatory to access Consolidated Fund of India benefits and file income taxes. Private companies, schools, banks and telecom companies could not make Aadhaar compulsory for their services.[89] Furthermore, the Court ruled that Aadhaar should not be compulsory for the University Grants Commission, the National Eligibility and Entrance Test, the Central Board of Secondary Education exams and school admissions. Despite this judgment, there are continued issues with Aadhaar being widely viewed and effectively treated as mandatory to access a range of services.[90]

Aadhaar has not been accessible or user-friendly for everyone. Authentication sometimes failed due to poor internet connections.[91] Persons whose fingerprints are worn or have had cataract surgery have trouble with the fingerprint and iris scan. Most estimates of ID system authentication failures are around five percent, but some estimates are as high as ten percent; either way, this is a

[85] *Puttaswamy v. India*, 2018, note 81, para. 266.
[86] Anirudh Burman and Suyash Rai, What is in India's Sweeping Personal Data Protection Bill?, 9 March 2020, Carnegie India. Available at: https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985.
[87] Human Rights Watch, India: Top Court OK's Biometric ID Program, 27 September 2018. Available at: https://www.hrw.org/news/2018/09/27/india-top-court-oks-biometric-id-program.
[88] *Ibid.*
[89] *Ibid.*
[90] State of Aadhaar, Top 10 Insights, available at: https://stateofaadhaar.in/top-10-insights.php; and Human Rights Watch, India: Identification Project Threatens Rights, 13 January 2018, available at: https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights.
[91] Human Rights Watch, *ibid*.

substantial number.[92] Certain marginalised groups have lower rates of Aadhaar enrolment; 30% of homeless persons lacked an Aadhaar number, perhaps because of the requirement to show residency.[93]

Other Key Concerns

Several other key issues with Aadhaar signal concerns to look out for with other digital ID regimes:

- *Data breaches*: Researchers and activists have identified a number of leaks of Aadhaar data or other breaches.[94] Many of these are related to attempts to link Aadhaar to other systems. For example, a failed attempt to link Aadhaar to voter registry lists has raised concerns about politicians accessing voter data.[95]
- *Surveillance*: Every time the Aadhaar system authenticates an identity, it stores that information in authentication logs. These logs have the potential to be used as a surveillance tool, which is of particular concern because the legal framework does not articulate clear standards for when law enforcement officials may access Aadhaar data.[96]
- *Oversight*: UIDAI was formed before the Aadhaar Act was passed, meaning that its legal mandate was created in an *ad hoc* fashion. The Supreme Court found that the grievance and appeals mechanisms were insufficient. Originally, the Aadhaar Act only permitted UIDAI to bring complaints about violations of the Act and not on behalf of individual victims. The Supreme Court has now directed that this should be amended, noting that the Act "does not place any institutional accountability upon UIDAI to protect the database of citizens' personal information."[97]

3.2 Kenya

Kenya's National Integrated Identity Management System (NIIMS) combines biometric data with personal information from pre-existing government databases. Ultimately, it aims to serve as the single source of ID in Kenya.[98] Upon registration, each person receives a unique number called a Huduma Number, or Huduma Namba in Swahili. The government has indicated that this will be necessary in order to access services in the future such as acquiring an ID card, passport or driving licence.

The government reported that 26 million Kenyans had registered in the first round of Huduma Namba registration, which ran from April to May 2019. The system uses information on nationality, place of birth, parentage, marital status, educational and employment background,

[92] Sushil Kambampati, note 78.
[93] State of Aadhaar, Top 10 Insights, note 90.
[94] SFLC, Aadhaar Breaches and Leaks, 24 April 2017. Available at: https://sflc.in/uidai-aadhaar-breaches-and-leaks.
[95] Aria Thaker, Data Leaks Could Wreak Havoc in India, So Why Aren't They an Issue this Election?, Quartz India, 4 April 2019. Available at: https://qz.com/india/1586748/data-leaks-and-cybersecurity-should-be-an-election-issue-in-india.
[96] Access Now, note 2, at 19.
[97] *Puttaswamy v. India*, 2018, note 82, para. 353 (directing amendment of section 47).
[98] National Government Communication Centre, Brochure: National Integrated Identity Management System. Available at: https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf.

disability and agricultural activities, but not race or religion, along with fingerprints and a photograph.[99]

In January 2020, the Kenyan High Court issued a constitutional judgment on NIIMS, halting its implementation until the government enacted a comprehensive regulatory framework, in particular relating to personal data protection.[100] The Kenyan High Court thus went further than India's Supreme Court.[101] Kenya did enact a Data Protection Act in 2019, which the Court found reflected "most of the applicable data protection principles" but still needed implementing regulations, accompanied by effective implementation and enforcement.[102]

The Court also expressed concern about data breaches and the need for strong security safeguards to protect data collected as part of the programme, stating: "It is our conclusion therefore that all biometric systems, whether centralised or decentralised, and whether using closed or open source technology, require a strong security policy and detailed procedures on its protection and security which comply with international standards."[103]

The Court did not find that NIIMS violated any equality or anti-discrimination standards, citing insufficient evidence, but it acknowledged that segments of the population might potentially be excluded (such as those who lack documents or biometrics). Accordingly, it emphasised the need for a clear regulatory framework to address the possibility that NIIMS would effectively be required to obtain social services, and the risk of some people being excluded.[104]

In practice, civil society groups have reported discrimination occurring throughout the ID distribution process, which involves a vetting committee with significant discretionary powers. Ethnic and religious minorities faced additional barriers when applying for biometric IDs and some were rejected outright; overall, ten percent of those who applied for a digital ID via NIIMS were denied due to lack of documentation.[105] This raises serious exclusion and discrimination concerns should Kenya proceed to link digital IDs to a range of other services, as it plans to do. In addition to satisfying the data protection concerns of the Supreme Court, Kenya may need to rethink the system for granting Kenyans digital IDs.

[99] Open Society Justice Initiative, Kenya's National Integrated Identity Management System, March 2020, p. 2. Available at: https://www.justiceinitiative.org/uploads/477c2588-00eb-4edd-b457-bf0d138fd197/briefing-kenya-niims-03232020.pdf.
[100] *Nubian Rights Forum v. Attorney General*, High Court of Kenya at Nairobi, Constitutional and Judicial Review Division, Consolidated Petitions No. 56, 58 & 59 of 2019, 30 January 2020. Available at: http://kenyalaw.org/caselaw/cases/view/189189/.
[101] Privacy International, Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons, 24 February 2020. Available at: https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons.
[102] *Nubian Rights Forum v. Attorney General*, note 100, paras. 1036-1037.
[103] *Ibid.*, para. 883.
[104] *Ibid.*, para. 1045.
[105] Wired, Digital IDs Make Systemic Bias Worse, 2 May 2020, available at: https://www.wired.com/story/opinion-digital-ids-make-systemic-bias-worse/; and The New York Times, Kenya's New Digital IDs May Exclude Millions of Minorities, 28 January 2020, available at: https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html.

3.3 Jamaica

Jamaica has sought to establish the National Identification System (NIDS) under the National Identification and Registration Act 2017,[106] among other things to enhance the efficiency of public services. The system relied on biometric data, including fingerprints, footprints and photographs,[107] to verify citizens' ID, based on a unique ID number for purposes of verification.[108] However, Jamaica's Constitutional Court struck down the Act in 2019,[109] requiring the government to develop new legislation for the system.[110]

In striking down the Act, the Court held that the "compulsory taking of biographical and biometric data" violated the right to privacy, which is protected under the Jamaican Constitution. The law did not employ a "data minimisation" approach, which would have met its objectives while collecting the minimal amount of data necessary.[111] Furthermore, the law lacked sufficient safeguards against the misuse of collected data, allowed for third party access to the database without adequate safeguards[112] and did not provide for independent oversight.[113]

The Court found it troubling that the National Identification and Registration Authority was proposing to give government control over large amounts of data without ensuring that individuals had the right to opt-out of the data collection. The judgment also expressed concern about a plan to link different silos of data together via a unique identification number; information about a single individual transaction might provide little insight into private behaviour but aggregating information about many transactions could provide a much deeper profile of an individual's behaviour. This could mean "reducing anonymity even further and increasing the possibility of profiling and generating new information about the data subject."[114]

4. Recommendations

Based on international human rights standards, constitutional decisions by leading national courts and challenges faced when implementing digital ID systems in other countries, we make the following recommendations for Myanmar as it considers a biometric digital ID regime:

---

[106] The National Identification and Registration Act (2017). Available at: https://opm.gov.jm/wp-content/uploads/2017/06/The-National-Identification-and-Registration-Act-2017-final-passed.pdf.
[107] Jamaica Observer, Implementation of National ID System a Must, 24 June 2017. Available at: http://www.jamaicaobserver.com/latestnews/Implementation_of_National_ID_system_a_must_%26%238211%3B_OPM.
[108] National Identification System (NIDS), Government of Jamaica. Available at: https://opm.gov.jm/portfolios/national-identification-system/.
[109] *Robinson, Julian v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 12 April 2019. Available at: https://supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica.
[110] Jamaica Observer, Gov't vows to push national ID system, 28 March 2020. Available at: http://www.jamaicaobserver.com/news/gov-t-vows-to-push-national-id-system_190837-2?profile=1373.
[111] *Robinson, Julian v. The Attorney General of Jamaica*, note 109, para. 250.
[112] *Ibid*., para. 251.
[113] *Ibid*., para. 249.
[114] *Ibid*., para. 237.

- A clear legal framework should be put in place before implementing any biometric digital ID regime. Digital ID systems represent a restriction on the right to privacy which, to be legitimate under international law, must be clearly based in law.[115] In addition, inadequate or non-existent legal frameworks create fertile ground for arbitrary application of the system, potentially breaching the right to privacy and leading to discriminatory impacts.

  The case studies highlight the challenges created by an inadequate legal framework, including legal challenges and confusing and inconsistent implementation. As evidenced by Aadhaar in India, a lack of clear rules can lead to poor protection against data breaches and confusion over which benefits should be linked to the digital ID regime.

- Myanmar should adopt a strong personal data protection law before putting in place a biometric digital ID regime or engaging in large-scale collection of biometric data. In addition to the legal framework for the biometric digital ID regime, strong privacy and data protection legislation is needed to protect users against abuse of the highly sensitive data involved.[116] In all three case study countries, courts determined that stronger data protection systems were needed to ensure appropriate implementation of digital ID regimes.

  Data protection regimes are complex. However, there are a number of good models for this in existence, including The European Union's General Data Protection Regulation. It is significant that the Regulation identifies biometric data as a distinct category of special personal data which requires heightened protection. European law also recognises that it is not legitimate to require private actors to retain personal data on a mass basis simply so that law enforcement officials can access that data later on should they wish to.

- Registration in biometric digital ID regimes should be voluntary and should not represent a pre-requisite for being able to access social services or benefits. Biometric data should only be collected with a person's consent. For this reason, digital ID schemes should never be mandatory, whether directly or indirectly, through conditioning access to key services on participating. As part of this, care should be taken to communicate clearly with users that having a biometric digital ID is not required to access social services.

- An independent oversight body should be established for any biometric digital ID regime, which could be the same as the oversight body for the personal data protection regime. This is crucial to ensure, in practice, that public authorities and private companies comply with the rules, including those aimed at protecting privacy. The independent oversight body should have a clear legal mandate and effective protection for its independence. Individuals should have the right to petition the oversight body for relief where they believe their privacy or other rights have been breached.

[115] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, note 29, para. 3.
[116] United Nations Development Group (UNDG), Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda. Available at: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.

- The system should be designed to ensure that private sector actors respect the privacy and other rights of users. The private sector is frequently involved both in the development and implementation of biometric digital ID systems and in the use of the authentication options they offer. Effective systems and safeguards need to be put in place to ensure that these private actors respect data protection and other rules aimed at protecting users, including systems to hold these actors to account for any breaches of the rules.[117] Private actors that process personal data should be obliged to establish internal mechanisms to ensure compliance, to issue data breach notifications in case of a breach, and to undertake privacy impact assessments.[118] To prevent discrimination, the rules should limit the sharing of biometric data to what is necessary to achieve legitimate objectives, such as the universal provision of services. Anti-discrimination laws should also be introduced to prohibit and penalise discrimination.

- Any biometric digital ID regime that is introduced in Myanmar should be based on residency rather than citizenship. Given the challenges regarding Myanmar's tiered system of citizenship, and the experience of other countries, any biometric digital ID regime should follow India's example and be based exclusively on residency rather than being linked in any way with citizenship status. India's example shows that a biometric ID system can be introduced much more efficiently when it is not tied to citizenship, which would require a more complicated review of documents for each individual. In addition, this approach ensures that all residents have a legal identity under the law, regardless of citizenship status. For similar reasons, the programme should not collect data related to citizenship status.

- A Myanmar digital ID scheme should not involve the collection of any data related to race, ethnicity or religion. The regime should also not collect data about ethnicity, race or religion since the risk of such data being misused outweighs any potential benefit from collecting it. None of the biometric ID systems discussed in the case studies collect such data and it is not necessary to create a legal ID system. As noted above, it is highly questionable whether such information should be included on paper IDs under international human rights law. However, when it comes to biometric data regimes the potential for abuse is even higher, given that such systems rely on central databases of immutable personal information. For this reason, even if ethnicity or religion is recorded on paper IDs, it should not be used in biometric digital ID regimes.

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of CLD and IMS and do not necessarily reflect the views of the European Union

[117] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, note 29, paras. 76-77.
[118] Report of the UN High Commissioner for Human Rights, note 19, para. 31.