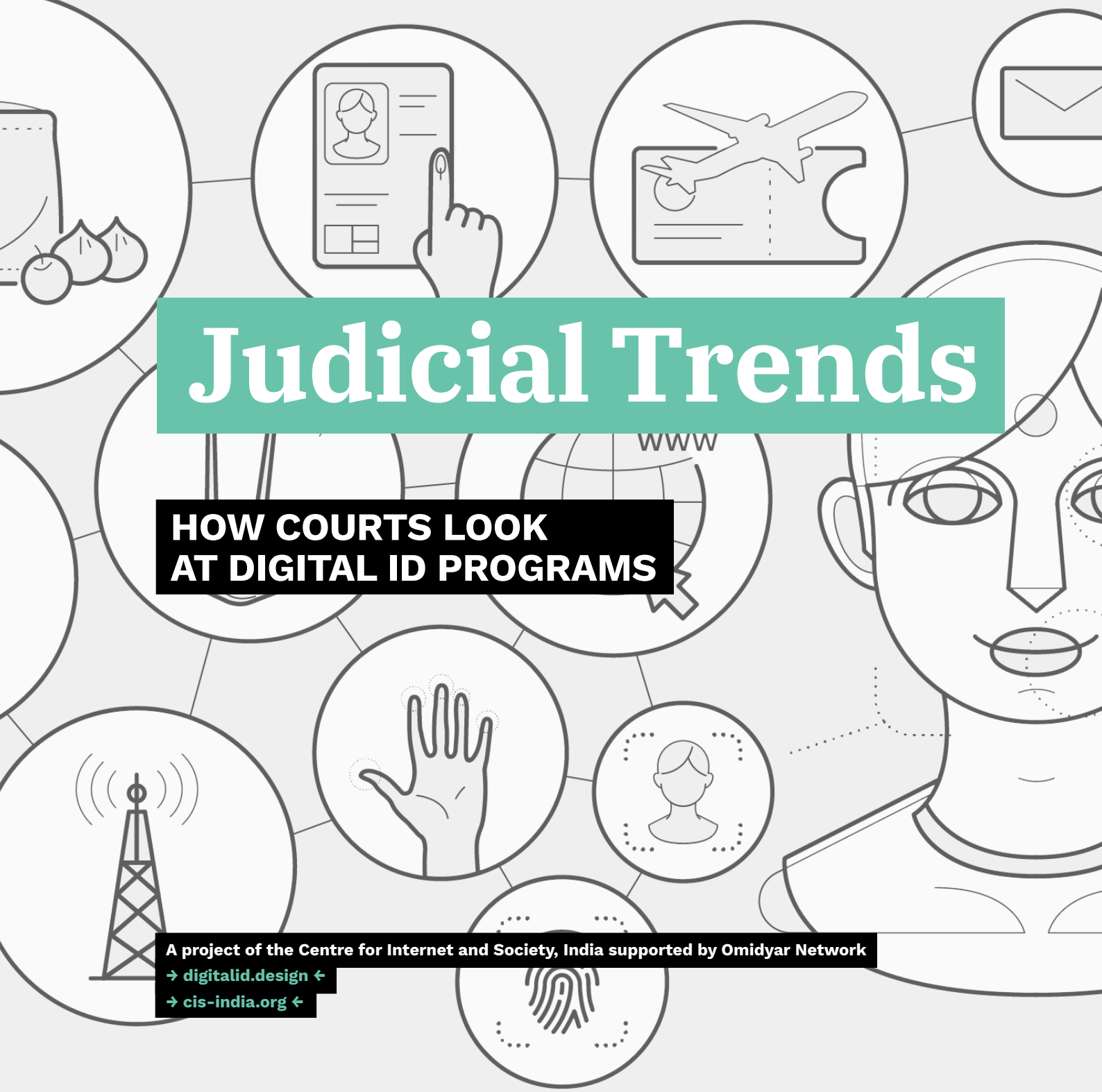

Judicial Trends

HOW COURTS LOOK AT DIGITAL ID PROGRAMS

A project of the Centre for Internet and Society, India supported by Omidyar Network
→ digitalid.design ←
→ cis-india.org ←

RESEARCH & WRITING
Shruti Trikanad

REVIEW & EDITING
Amber Sinha and Anubha Sinha

DESIGN
Pooja Saxena

LAYOUT & COVER ILLUSTRATION
Akash Sheshadri

THE CENTRE FOR internet & society

INTRODUCTION

The insurgence of technology in nearly all aspects of an individual's life has made its inevitable way to governance. National digital ID systems are being adopted worldwide by governments as reliable means to identify residents and provide them with services they are entitled to. This however, is also following a noticeable pattern — developed liberal democracies have been rejecting such systems as far back as the early 2000s,[1] while developing nations are increasingly embracing them in more recent years.[2] Some among the latter have seen these systems come to the forefront of their politics, with their apex courts determining their constitutionality and future. These ID schemes have been challenged for the various constitutional threats they posed to the users subjected to them. Although varying in design and reach, they introduced similar risks in their populace, that came only from replacing governance with invasive technology.

We have engaged in a study of the different issues that these courts were tasked with adjudicating, in a hope that it will provide insight into the nature of Digital ID systems and their interplay with constitutional protections. These courts identified the risks of the system, the trade-offs they introduced, and how they could be potentially altered to serve their purpose while limiting harm. In this series, similarities, differences, patterns, and exceptions will be highlighted, with the goal of understanding better how and why these ID systems were endorsed, discontinued, or limited by courts. In the next few pieces, we will analyse the final outcomes in the judicial challenges, and what factors were considered in the privacy tests to arrive at such outcomes, as well as how technological issues were handled by the courts.

We are looking at four Digital ID judgments here. While several cases have been heard by courts on aspects of privacy and biometric databases worldwide, only these four were about foundational national Digital ID systems. Foundational systems are core identity systems catering to the general public, created to provide identity proof for a variety of services.[3] They differ from biometric databases because they provide credentials to the ID holders to validate their identity, and from other Digital ID systems because they are not limited to one

1 See the debates surrounding the National Identification Scheme in the U.S. and the Identity Card Act, 2006 of the UK.

2 See upcoming ID systems in Nigeria, Pakistan, Thailand, Peru etc

3 "Core Concepts and Processes", Digital Identities: Design and Uses, Centre for Internet and Society, last accessed June 9, 2020, *https://digitalid.design/core-concepts-processes.html*

function or use.[4] The national ID systems in India, Jamaica, Kenya, and Mauritius sought to provide a digital identity to residents for a variety of purposes not restricted to a single sector.* In all of these cases, privacy issues were enhanced by the use of biometric factors and technology in the creation of verifiable identities.

*Details of these ID systems and the litigation surrounding them can be found on page 47.

At the outset, the following are the key factors we determined to affect the outcome of the case:

1. The contours of the ID system and its legal framework
2. The Constitution and scope and substance of rights
3. The court in which it was adjudicated (High Courts/Supreme Courts) and nature of the adjudication process
4. The petitioners, the claims, and the defence of the respondents (many issues were expressly not adjudicated upon because the petitioners did not make claims)
5. The judges, their experience with the subject matter, and prior similar cases they might have heard
6. The stage of the digital ID project
7. The constitutional governance structure, separation of powers, judicial deference, and power of judicial review.
8. The adversarial nature of the trial, evidence, use of expert testimony.
9. The existence of prior precedents (around the world)

4 "Core Concepts and Processes", Digital Identities: Design and Uses, Centre for Internet and Society, last accessed June 9, 2020, *https://digitalid.design/core-concepts-processes.html*

CONTENTS

SECTION I.
PRIVACY AND IDENTITY

Undoubtedly, the biggest risk of a national Digital ID program is its impact on the privacy of citizens. Individuals are coerced into parting with their privacy, right from divulging personal information to get enrolled into the program, to being monitored at their every interaction with the ID. While some of these concerns may be termed only "risks," because of the plausibility of their occurrence — such as the collected data being hacked by third parties — other concerns are certain, such as the State having access to personal and biometric data. It also becomes important to note that the privacy risk in question far surpasses that of such personal data being shared with the State; in the use of a nation-wide pervasive digital ID scheme, privacy violations can occur in several other ways: by keeping records of every instance of authentication of ID by the user, the State is able to monitor the ID holder's every transaction and action: this is a disclosure of (personal) information that is made without the consent, and often the knowledge, of the individual; by enabling linking of various databases through a unique ID, the State, or any private actor accessing such information, can identify new information about the interests, personality, actions, political leanings etc of the individual, which they did not consent to share; by not providing sufficient security measures for the data collected when in storage, the individual can no longer adequately ensure control over the personal information they shared while obtaining the ID, which they only consented to share with the *State*; by allowing easy legal access of the collected information, or frequent disclosures to State bodies, the individual entirely loses control over their own data. In this way, Digital ID programs pose several privacy risks of differing severity and plausibility, all in all making them dangerous tools of governance unless properly regulated.

An examination of the cases shows that the courts' adjudication of privacy issues can be categorised into: the collection of biometric information, the collection of authentication/transaction information, the design or architecture of the system, and the legal framework of the system governing the use and further disclosure of data. Due to the varying stages of development and implementation of the ID systems in the States selected for this study, some of the privacy issues were not decided upon by the courts, as they were deemed to be premature. Eventually, the final outcome was largely a determination of whether the ID system's benefits and/or purposes were proportional to its infringement of constitutional rights.

Where the Privacy Issue Lies

The privacy risk of submitting large swathes of data — often including biometric data — to the State is common to different ID systems, but differs based on many factors endemic to the concerned State. Privacy is considered a fundamental right in most States, either expressly in their Constitutions,[5] or interpreted into other Constitutional rights.[6] Across all these jurisdictions, there was no doubt that digital ID schemes violate or threaten to violate these fundamental freedoms; the only disparity lay in what elements of privacy may be harmed, and what ought to be protected.

Informational Privacy

The **Indian** Supreme Court, in *K.S Puttaswamy v. UoI* ("**Aadhaar Case**"), was tasked with determining whether the national digital ID project, titled Aadhaar, was unconstitutional. To do this, they had to first establish a fundamental right to privacy in the Indian Constitution. The fundamental right to privacy was found to be ingrained in all the fundamental rights accorded by the Constitution, and particularly the right to life. It was held to comprise primarily three aspects - (i) intrusion with an individual's physical body, (ii) informational privacy, and (iii) privacy of choice.

Justice Chandrachud perhaps best defined informational privacy as "*control a person has over dissemination of information that is personal to them.*"[7] He identified the harm caused by a disclosure of *information*, one that is distinct from the other aspects of privacy, when he described the impact of the electronic trail left behind by users of the internet[8] — the information contained in these tracks allow an observation of the sort of the person that the user is, and their interests.[9] When aggregated, such information is a powerful indication of their personality, even when it is not explicitly disclosed and may better remain hidden. Oftentimes this leads to the creation of *new* information about an individual that was never

5 See the constitutions of Kenya, Jamaica, Canada, Germany etc.

6 See the Indian Constitution and its interpretation in *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 10 SCC 1 (2017).

7 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 10 SCC 1, (2017) ¶ 521 (Nariman, J.)

8 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 10 SCC 1, (2017) ¶ 300 (Chandrachud, J.)

9 See Francois Nawrot, Katarzyna Syska and Przemyslaw Switalski, "Horizontal Application of Fundamental Rights — Right to Privacy on the Internet", *9 Annual European Constitutionalism Seminar, University of Warsaw* (2010).

revealed. Perhaps even more concerning is the creation of "big data" comprising many data sets that are capable of being searched and linked to one another.

In the Aadhaar case, petitioners claimed that informational privacy was being severely breached in two respects. First, in the identification stage, when collecting large amounts of demographic and biometric information from residents, and from mandating the linking of an Aadhaar number holder's bank account, sim card, PAN number etc. Second, at every authentication by the Aadhaar holder, for every transaction they enter into, the following information was collected:[10] Aadhaar number, name of Aadhaar holder, whether authentication failed or was successful, reason for such failure, requesting entities' Internet Protocol (IP) address, date and time of authentication, device ID and its unique ID of authentication device which can be used to locate the individual. The information created at every authentication also has the effect of reporting to the government the actions of the Aadhaar holder (where Aadhaar is involved). J. Chandrachud captured the apprehension of this with what he identified as "'veillant panoptic assemblage' — where data gathered through citizens' ordinary practises, especially using something that had become as ubiquitous as Aadhaar, finds its way to State surveillance mechanisms.[11]

The Aadhaar case resulted in a majority opinion, and a dissent by J. Chandrachud. The majority held that while informational privacy formed an important part of the constitutional right of privacy, the extent of privacy that warranted protection depends on an individual's "reasonable expectation of privacy". This, in turn, requires the individual to show a "likely and real" harm that may be inflicted on them on account of the alleged privacy-impacting act, that is not "flimsy or trivial" but reasonable.[12] For Aadhaar, they held that the demographic and photographic information collected in the issue of the ID are widely collected by many other governmental bodies, and thus do not accord special privacy protection in this case. Even the core biometric information comprising fingerprints and iris scans are the *minimal* data collected for enrolment; thus, as per their balancing test, this sacrifice to their right to privacy is balanced against the purpose for the disclosure of information (and the data subject's right to seek benefits of the welfare scheme). The intent of the judges here is unclear, but implicitly it would seem they recognised that the sharing of core biometric data is an infringement of informational privacy, albeit one that

10 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 170 (Sikri, J.)

11 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 305.

12 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 359 ¶ 289.

is permitted by an interpretation of the Indian fundamental right to privacy. The court was also tasked with determining whether personal data about individuals that becomes known when they authenticate their Aadhaar ID — authentication information — impacts their right to informational privacy. The court opined that since only limited identification data was shared on authentications, and data collected at enrolment is minimal with specific exception of data concerning religion, caste, tribe, language of records of entitlement income or medical history, there was no risk of finding any new information that would threaten the ID holder's informational privacy rights.[13]

In **Jamaica**, their National Identification and Registration Act ("**NIRA**") was challenged in *Robinson, Julian v. the Attorney General of Jamaica*, for endangering Jamaicans' privacy. Before addressing the substance of the petitioners' claims, the Supreme Court adjudicated on the nature and scope of "privacy" that was accorded constitutional protection. The fundamental right to privacy is contained in Article 13(3)(j) of the Constitution, and amongst other things includes an obligation on the State to respect an individual's "private and family life."[14] The court interpreted this as ensuring a right to informational privacy. Chief Justice Sykes observed that in a free and democratic society, privacy recognises that "a person's biometric information is theirs and that they retain control over that information by virtue of their inherent dignity as free autonomous beings"[15] Accordingly, they are free to decide whether their demographic/biometric information is shared, and under what circumstances. This endorses J. Chandrachud's view of informational privacy, as the control a person retains over their personal information. Additionally, it differs from the treatment of the Aadhaar majority towards informational privacy, insofar here there is no determination made of whether there was a "reasonable expectation of privacy," and ultimately the crux lies in whether the individual exercised control over the dissemination of their information. J Sykes also made the timely observation that privacy cannot be abrogated because "honest citizens have nothing to fear", because in a democratic society, individuals retain control over their body, home, mind, heart, and soul. In the scheme of a Digital ID program, it is more so concerning because of the use of a unique identifier that can link data about a person across different databases. This, once again, was a divergence from the

13 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶¶ 297 onwards.

14 Article 13(3)(j), The Constitution of Jamaica, 1962.

15 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 184, ¶ 10.

Aadhaar majority, as the court recognised that it was not individual categories of data that had to be examined for a privacy claim over it, but the *aggregation* of all such categories of data that posed the real privacy harm.[16]

Eventually, on completing the proportionality test, the court held that the entire scheme ought to be shut down for its unconstitutionality because the current governing framework does not accord sufficient protection to the data collected through the scheme.

In **Kenya**, the High Court of Kenya decided on the constitutionality of their digital ID scheme titled *Huduma Namba*. Although currently being appealed, the judgment provides important insight into how the use of *Huduma Namba* is likely to lead to breaches of privacy of residents. The court held that a right to privacy envisages the right to "*live one's life with minimum interference.*"[17] What is important to note is that this court categorically recognised that the right to privacy does not pertain merely to information that could be damaging to the dignity or reputation of an individual if revealed, or in any manner cause harm on disclosure, but accords protection to all private information so as to allow the individual to retain control over its dissemination.[18] This, once again, is a departure from the Aadhaar majority's interpretation. "Private information", in turn, is not merely information that is considered intimate, that the individual would rather shroud in secrecy, but other information that they consider private, even if pertaining to their presence or actions in a public place.[19] However, since the petitioners only brought claims regarding biometric and GPS data, both of which would be considered private information according protection even by the Aadhaar court's test, the court's conviction in protecting all private information was never really put to test.

The right to privacy is codified in Article 31 of the Kenyan Constitution and comprises, inter alia, a right "*not to have information relating to their family or private affairs unnecessarily required or revealed.*"[20] This right can be abrogated if done by law, and to the extent the limitation is "*reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.*"[21] This, in the court's assessment, constituted the right to informational privacy. Thus, it had to consider 2 aspects: first, if the collection of data entailed in the *Huduma*

16 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 36 of (B) of 247 (Sykes, J.)

17 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 750.

18 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶¶ 749-750.

19 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 750.

20 Article 31(c), The Constitution of Kenya, 2010.

21 Article 24(1), The Constitution of Kenya, 2010.

Namba scheme violated an individual's right to informational privacy; and second, if it did, was it a permissible limitation. In considering the first aspect, the court examined if the information collected was required or necessary, as well as whether the protection accorded to it by the data protection framework ensured that the information would not be further revealed (as that would constitute an independent breach of informational privacy by the State). First tasked with determining whether biometric information could be regarded 'private information' that deserved constitutional protection, the court held that information about "*their (individuals') unique human characteristics*" which "*allow them to be recognised or identified by others*" is private information as it is data about "one's body, presence, image and identity, in both private and public places."[22] Accordingly, they held that biometric data was personal information subject to Article 3 protection.[23] The next question that needed addressing was whether the collection of biometric data was *necessary*.[24] The petitioners argued that there was no stated purpose of the *Huduma Namba* scheme, and therefore the collection of biometric data was purpose-free.[25] They also challenged the utility of biometric data itself, for identification of persons, based on expert testimony that claimed that there would be difficulties in accurately ascertaining some biometric features (such as worn fingerprints), and that biometric authentication was probabilistic and could therefore lead to false conclusions and insufficient deduplication of data.[26] The court held that the *purpose* of the collection of biometric data was for the "identification of natural persons," and to that extent it is necessary for identification purposes.[27] Relying on the Article 29, Data Protection Working Party in its Working Document on Biometrics, it also held that due to the universalistic, unique, and permanent nature of biometric data, they were suitable for authentication and verification purposes.[28] It was only with regard to DNA information, that the Respondents admitted they were unable to process for the entire population in a manner that would make them usable for authentication, that the court held was unnecessary with respect to Article 31. Additionally, the collection of GPS monitors, which posed the problem of allowing real time surveillance of individuals, was also considered unnecessary, particularly in light of the Respondent's admission of its inability to collect.[29]

22 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 750.

23 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 758.

24 Article 31(c), The Constitution of Kenya, 2010.

25 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 774.

26 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 775.

27 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 786.

28 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 778.

29 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 781.

The court went on to hold that it was necessary to collect several biometric characteristics, as a multi-modal identification system would help improve the performance and accuracy of NIIMS.[30] This was more so true because all individuals may not possess every required biometric characteristic.[31] Since the purpose of the *Huduma Namba* exercise was to establish a digital database that would be a "single source of truth,"[32] it was principally an identification and verification system, and to that extent the collection of personal information was necessary. Thus, apart from DNA and GPS coordinates, the information collected pursuant to *Huduma Namba* was considered necessary and therefore constitutional. The court also made an important deviation from its counterparts in India and Jamaica here; it held that even though most of the personal information was collected with individuals' consent, since it was pursuant to the newly enacted Data Protection Act, it was still subject to a privacy analysis. It categorically held that the collection of personal data was done with data subjects' consent (based in part on the petitioner's inability to present evidence of persons being forced to give consent), and proceeded to evaluate the intrusiveness of the amendments and their impact on privacy by the test of *relevance*. On the contrary, the Indian court only assessed potential privacy violations in the collection of personal information under Sections 7 and 8 of the Aadhaar Act, where obtaining Aadhaar is mandatory to access certain public services, ignoring the privacy concerns of other Aadhaar holders. Similarly, since the ID was mandatory in Jamaica, the Jamaican court only considered the potential privacy violations of collecting biometric data *without consent*.

The second important assessment was whether the legal and institutional framework surrounding NIIMS was adequate to protect individuals from a further unnecessary disclosure of their personal information. For this, petitioners argued that the laws governing NIIMS, its technological and architectural design, and the paucity of information on its security features, all contributed to an inadequate framework to protect privacy. They also argued that the interoperability of NIIMS — that allowed various Ministries, Departments and State agencies to directly access NIIMS for purposes of authentication of identity — was unnecessary and posed an additional privacy risk.[33] However, the court refused to engage on issues that it considered were policy decisions or about the technological design of the system. It restricted itself to an assessment of the legal

30 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 781.

31 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 782.

32 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 785.

33 Third party access could be entirely removed by instead requiring direct authentication from the central NIIMS database. See *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 859.

data protection framework governing NIIMS. It held that while a data protection framework was in place, data protection principles and standards should be categorically provided in regulations governing NIIMS, and adequately *actualized* in its operation.[34] To that extent, it found the legal framework lacking and posing serious risk to the security of data in NIIMS. Thus, in light of the risk it invites for data breaches and unauthorized access, it was a limitation to the right to privacy found in Article 31(c).[35] The constitutionality of the scheme therefore hinged on whether such a limitation was justifiable in a democratic society.

In **Mauritius**, the only private information that was considered, in the petition and in the judgment, was that of the biometric data extracted. The court only looked into its impact on bodily privacy, and did not consider informational privacy an issue.

Autonomy of Choice

In **Jamaica**, the fundamental right to privacy is contained in Article 13(3)(j) of the Constitution. It comprises a right to be protected from "*search of the person and property*", a respect for "*private and family life*" and a protection of privacy of other property.[36] Here, while examining the impact of NIRA on this right, they found that it was the *mandatory* collection of data, along with inadequate protection of such data, that impacted their privacy rights. However, in addition to this right, the court leveraged principles embedded in the constitution such as the obligation to respect the inherent dignity of individuals,[37] and respect them as "citizens of a free and democratic society"[38] to interpret a right to have "privacy of choice". Even notwithstanding the right to privacy they held that a right of individuals to "decide what to do with their own privacy" inhered in the fundamental right to life, liberty, and security found in 13(3)(a) of the Constitution of Jamaica.[39] The mandatory nature of NIRA, requiring individuals to part with their biometric and biographical information at the risk of criminal sanction, impacted this right.[40] The judges also identified that this was not identical to simply the State collecting data without consent, because the use of a single

34 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 884.

35 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 920.

36 Article 13(3)(j), The Constitution of Jamaica, 1962.

37 Article 13(1)(a), The Constitution of Jamaica, 1962.

38 Article 13(1)(b), The Constitution of Jamaica, 1962.

39 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 189, ¶ 18 (Sykes, J.).

40 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 189, ¶ 19.

number linking together different databases allowed new information to be generated that was neither contemplated nor consented to by the individual.[41]

Although the petitioners in the Aadhaar case in **India** argued that individuals must be allowed the choice of their preferred mode of authentication, the court failed to engage in their decision. However, the court, in its interpretation of "dignity," opined that in welfare States, fundamental right to minimum living conditions formed the core of personal autonomy, as individuals must be "free from want" to be truly autonomous; this, it seemed to think, was unobtainable without Aadhaar.[42] Similarly in **Mauritius**, the petitioners claimed that by mandating possession of the ID, their right to choose, subsumed under their right to liberty, was violated, but the court held that the Mauritian right to liberty only extended to physical liberty, which was not impacted by the ID. Autonomy, as a facet of privacy, was neither claimed nor addressed in the **Kenyan** case.

Anonymity

Anonymity may not seem like a particularly essential right to accord to individuals, but its significance is heightened because of the nature of digital ID programs. The collection of large swathes of demographic and biometric information, along with records of ID holders' actions and transactions, all linked to each other by a unique number, essentially strip away any semblance of anonymity of an ordinary individual. An actor with access to any part of this system and armed with limited information about the ID holder can easily find them and generate new information about them without their knowledge. However, this did not form a substantial part of the claims or the judgments in these cases, with the exception of Jamaica.

The **Jamaican** Supreme Court, in Robinson, included the right to anonymity in their description of privacy.[43] J. Sykes identified as a feature of free and democratic societies the right of the individual to be "as anonymous as possible."[44] Although the right to privacy as codified in the Jamaican Constitution[45] does not include any right to anonymity, its scope was expanded after consideration of the Canadian Supreme Court's assessment of its own

41 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 190, ¶ 20.

42 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 200, ¶ 116.

43 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 184, ¶ 10 (Sykes, J.).

44 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 184, ¶ 11 (Sykes, J.).

45 Article 13(3)(j), The Constitution of Jamaica, 1962.

Charter right[46] against "unreasonable search or seizure."[47] The Canadian Supreme Court described the right to anonymity as that of individuals to "act in public places but preserve freedom from identification and surveillance," and found that it has become particularly important in the context of internet usage.[48] Consequently, the Jamaican court held that the mandatory collection of biometric and biographical data leads to a complete elimination of the anonymity of individuals, and for that reason, amongst others, violates the fundamental right to privacy found in 13(3)(j) of the Constitution.[49]

Bodily Privacy and Search of Home, Property and Body

The **Jamaican** Constitution expressly protects individuals' right against "search of person and property."[50] Relying on a Canadian case[51] that interpreted an identical right in the Canadian Charter,[52] the court understood this provision as protecting personal information that "*individuals in a free and democratic society would wish to control from dissemination to the State.*" In particular, this would involve biometric and biographic data, as they are able to reveal intimate details about the individual.[53] In effect, a mandatory collection of biographical and biometric data is a violation of bodily privacy protected in 13(3)(j)(i) of the Jamaican Charter.[54]

The respondents in this case argued that bodily privacy was not being harmed by NIRA because there was no assault in the collection of biometric data. However, the court categorically held that the threat of criminalization to get citizens to give up their biometric information was sufficient to violate this right.[55]

In **Mauritius**, the Supreme Court was hearing the challenge of their National Identity Card scheme that used a biometric smart card to accord legal identities to residents.[56] The petitioners challenged the mandatory collection of fingerprints

46 Article 8, The Canadian Charter of Rights and Freedoms, 1982.

47 *R v. Spence* [2014] 2 SCR 212.

48 *R v. Spence*, [2014] 2 SCR 212.

49 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 201, ¶ 38.

50 Article 13(3)(j), The Constitution of Jamaica, 1962.

51 *R v. Plant* [1993] 3 SCR 281.

52 Article 8, The Canadian Charter of Rights and Freedoms, 1982.

53 *R v. Plant*, [1993] 3 SCR 281.

54 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 201, ¶ 38.

55 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 209, ¶ 61.

56 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177.

and demographic data on many grounds, including of violating liberty, freedom, non-discrimination [...] rights of individuals, etc, but were unsuccessful. The only issue the court engaged with was its potential violation of the right against "search of person or property" without consent.[57] The court had to determine whether the extraction of fingerprints — at the threat of criminal sanction — amounted to a search of their person. It observed that the collection of biometric information included the extraction of minutiae from fingerprints, and encoding them to record in the register.[58] This minutiae contain unique personal data peculiar to each individual. Adopting a purposive interpretation to the Constitution, the court held that the collection of biometric information without consent violated this fundamental right. The protection against search of a person was not limited to a search of the *whole body* of a person,[59] but extended to an undue intrusion or inspection of any part of the body.[60] Regardless of the purpose for the intrusion, or the degree of intrusiveness, the coercive taking of fingerprints of persons and extracting their minutiae amounts to a violation of the privacy right protected by the Constitution.[61]

Although claimed by the petitioners in the cases in **India** and **Kenya**, both courts failed to address the issue of bodily privacy as a facet of privacy. This could be attributed to the fact that the "right against search," which was the determinate right in the above mentioned cases in Jamaica and Mauritius, did not form a part of the Indian or Kenyan constitutions.

Elements of a Digital ID Scheme that Impact Privacy

Although the impact of Digital ID schemes on individuals' privacy was undisputed, courts differed slightly on what aspects of a digital ID program triggered such privacy claims. An examination of this will comprise all those elements that threatened to impact privacy rights, regardless of whether they were eventually held unconstitutional (based on a proportionality analysis or a consideration of the surrounding legal framework). We have only included within each section those cases that considered the particular aspect highlighted to be a potential privacy violation.

57 Section 9(1), The Constitution of the Republic of Mauritius, 1968.

58 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 22.

59 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 22.

60 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 23.

61 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 22.

Mandatory Collection of Biometric Data

The State wide collection of individuals' biometric data was the driving force behind the courts' engagement with issues of privacy.[62] It only bears mention here as an important element of a digital ID scheme that is considered to threaten the privacy rights of ID holders.

In **India**, Aadhaar was made mandatory for beneficiaries seeking certain government services and benefits,[63] and largely voluntary for the rest of the populace.[64] Although the petitioners argued that both these cases should be assessed for their privacy impact, the court only discussed the privacy rights of those for whom Aadhaar possession was mandatory. Thus, when it came to the collection of data, it only concerned itself with the collection that was done without consent of the ID applicants. As has been discussed before,[65] the court eventually held that since the data collected was minimal, it was not a disproportionate violation of privacy.[66] However, implicit in this judgment is the recognition of the impact that collection of biometric data has on the data subject's privacy; it does threaten a subject's privacy rights, but in a manner that was proportional and necessary for the attainment of other fundamental rights, thereby achieving constitutionality.

In **Jamaica**, Section 20(1)-(7) of the NIRA mandates every registerable individual to apply for enrolment in the database. This mandate was enhanced by two important consequences for not registering- first, delinquents were threatened with criminal sanctions. Second, most government services were obligated to mandate the ID before offering any services to residents. The court held that it was the failure to require consent in collection of information that was unconstitutional, because it entirely eliminated the right of the individual to choose whether or not they wanted to share personal information.[67]

In **Mauritius**, the Supreme Court held that the coercive taking of fingerprints from Mauritius citizens and extracting their minutiae, violates the protection against the "*undue interference by way of a search of any part of the body of a person*

62 See 'Informational Privacy' and 'Bodily Privacy' sections above.

63 Section 7-8, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

64 This was effectively diluted by the Finance Act 2017 which introduced Section 139AA to the Income Tax Act, 1961 and made it mandatory to quote an Aadhaar number while filing income tax.

65 See 'Informational Privacy' section above.

66 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 295.

67 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 38.

without his consent" found in Article 9(1) of the Constitution, and therefore violates their right to privacy. This is regardless of the level of intrusiveness of the collection process, and is a categorical feature of the right itself.[68]

In **Kenya**, although the initial collection of data for the issue of the *Huduma Namba* was done without requiring consent of the data subject, since the amendment (under litigation) was passed, and with the newly operational Data Protection Act, 2019, individuals' consent had to be sought before collecting their data.[69] The court had also, in a previous order,[70] ruled that this collection of data cannot be made mandatory. Although the petitioners claimed that the consent was not *informed*, as there was some discrepancy on the registration form given to applicants, the court held that in the absence of evidence of persons forced to give consent, they could not hold otherwise. As a result, the court only looked into privacy concerns arising from a consensual collection of biometric data.[71]

Third Party Access to Data

Although purportedly created for individuals to be able to prove their identity to the State, most ID systems also permit private parties to use the identity system for their own ends. Besides increasing the actors who have access to personal information, this also widens the reach of the ID system into an individual's life, and potentially eases deeper surveillance.

In **India**, Section 57 of the Aadhaar Act, which allowed the authentication mechanism of Aadhaar to be used by any private party pursuant to any law or contract, was a primary challenge of the petitioners in the Aadhaar case. It was claimed to allow an unrestricted extension of the Aadhaar platform to *any* user, and easily allowed Aadhaar seeding into several service provider databases.[72] The court, agreeing with the severe privacy harms that such a system entails, held that the provision fails the proportionality test and is consequently unconstitutional.[73]

68 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 23.

69 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 765.

70 *Nubian Rights Forum & Ors v. Attorney General of Kenya & Ors.* [2019] High Court of Kenya, Ruling No. 3, available at *http://kenyalaw.org/caselaw/cases/export/172447/pdf*.

71 See 'Informational Privacy' section above.

72 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 358

73 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 366 (Sikri, J.). This position was amended by the Aadhaar 2019 amendment Act.

In **Jamaica**, the court held that Section 39 of NIRA, which permits third parties to have access to the Database for verification purposes, violates the right to privacy found in section 13 (3) (j) (ii). It also observed that there were no justifiable reasons tendered for why third parties must have access to the database for authentication, when the purpose of the Act was for accessing government services.

Additionally, the complete lack of safeguards or governance for use by third parties alarmed the court. Sec 39 allows requesting entities to use authentication services of the authority, without specifying what information can be shared and/or recorded by the RE. There is no prohibition on storing data by Requesting Entities. There is also no need to get the consent of the individual before verifying their identity. By failing to address matters of data retention periods and treatment of authentication records, NIRA violated the privacy rights of Jamaican residents.[74]

In **Mauritius**, access to data collected under the NIC Act is governed by the Data Protection Act ("**DPA**"). Under the DPA, data can be processed only subject to express consent of the data subject.[75] This does not in any manner restrict third party access to data, provided the data subject consents to such access. Express consent need not be sought, however, when processing is needed "for the performance of a contract to which the data subject is a party", "for compliance with any legal obligation to which the data controller is subject" and "in the public interest".[76] This easy access to personal data collected under the Act was held to be a violation of privacy that is not "reasonably justifiable in a democratic society."[77]

Disclosures

Most Digital ID schemes permit disclosures of personal data collected under it, for several reasons, typically associated with national security, prevention of crime, compliance with judicial orders, etc. These are reasons often entirely detached from the purpose of the ID system itself. Disclosures are usually managed by the administrator of the system, without the consent (or often participation) of the ID holder.

74 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 359.

75 Section 24(1), Data Protection Act, 2017.

76 Section 24(2), Data Protection Act, 2017.

77 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 34.

In **Jamaica**, section 43 of the Act allows the authority to disclose identity information in the database in the following circumstances:

a. Pursuant to a request of the individual whose identification is being disclosed;

b. To facilitate the identification of the bodies of unknown deceased persons;

c. To facilitate the finding or identification of missing persons; *or*

d. Where the Act authorizes the disclosure

Additionally, identity information may be disclosed by a court, on an *ex-parte* application by the Authority:

a. For the prevention or detection of a crime;

b. In the interest of national security;

c. Where there is a public emergency; or

d. To facilitate an investigation under the Proceeds of Crimes Act.

The court held that these vague provisions facilitated violation of individuals' privacy because of the broad terms for allowing disclosures, with little or no oversight. Specification of terms for these disclosures are also left to regulations, which have not (yet) been made. This was held to be an unconstitutional infringement of individuals' privacy rights.[78]

The court in **Mauritius** analysed the disclosures permitted under the Data Protection Act, applicable to the data collected under the NIC Act. Disclosures are easily allowed under the DPA, for reasons ranging from national security,[79] to the prevention of crime and the assessment of tax,[80] in relation to the health of the individual,[81] to if the disclosure is necessary for obtaining legal advice.[82] The low threshold for permitting disclosures, together with the complete lack of judicial oversight to monitor such disclosures, was concerning to the court, prompting them to hold that such uncontrolled access without sufficient safeguards was an unjustifiable violation of citizens' right to privacy.[83]

78 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 367.

79 Section 45, Data Protection Act, 2017.

80 Section 46, Data Protection Act, 2017.

81 Section 46, Data Protection Act, 2017.

82 Section 52(3), Data Protection Act, 2017.

83 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 34

In **India**, the Aadhaar court looked at the constitutionality of the Aadhaar Act which allowed identity information and authentication records to be disclosed to relevant authorities on judicial orders, or in the interest of national security.[84] While ultimately declaring the provision constitutional as it was a legitimate exception under the fundamental right to privacy, the court identified the privacy harms involved in such disclosures by limiting the scope of the provisions, and ensuring more judicial oversight and control by the data subject.[85]

Linking of Different Databases

Digital ID systems are often championed for their interoperability, created by linking together different databases and seeding users' unique ID into them.

The Aadhaar bench in **India** was tasked with determining whether the seeding of Aadhaar in the Permanent Account Number ("PAN") database — ergo a linking of the two databases — was constitutional. The court held that in a social welfare State, ensuring optimum distribution of scarce public resources was a legitimate aim of the State and fulfils the proportionality test for a violation of the right to privacy.[86] However, they held that a mandatory linking of the Aadhaar number with bank accounts,[87] and with mobile numbers,[88] was unconstitutional as it failed the proportionality test. Here, the court did recognise the privacy threat introduced by linking databases, but perhaps not as clearly as the petitioners, for whom the issue of Aadhaar seeding took almost the forefront of their case.

In **Jamaica**, the National Identification Number (NIN) was to be embedded in all government databases to enable their easy linking. The judges recognised that this created a novel privacy risk, unique to a Digital ID system and different from that of simply collecting and storing the same data, since this allowed actors to query the database and easily single out specific individuals; this is especially harmful, as among the data linked is the biometric information of individuals, such that biometric particulars can also be identified through this linking process.[89] The power that this would give the State, to analyse and generate new

84 Section 33, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

85 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶¶ 342-349 (Sikri, J.).

86 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 425 (Sikri, J.).

87 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 436 (Sikri, J.).

88 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 442 (Sikri, J.).

89 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 189, ¶ 20.

information about its citizens, harmed individuals' privacy rights and warranted extra protection. Additionally, they observed that there were no statutory provisions proscribing profiling by the State,[90] and in fact the "compiling and reporting statistical information derived from analysing the information stored in the Database"[91] was explicitly permitted by the NIRA. The judges also opined that a linking of databases through a unique identifier would lead to far greater damage caused by unauthorized access or hacking.[92]

The NIIMS database in **Kenya** envisioned the linking of several different government databases for the purposes of deduplication and verification of personal data contained in them. The petitioners argued that this interconnected web of databases will allow the NIIMS databases to access information stored in functional databases, and lead to invasive and prejudicial searches.[93] For its part, the court recognised that the process of linking information across different databases put data subjects at an amplified risk of unauthorized access and surveillance, increasing further the risk of use of data for unintended purposes.[94] However, it refused to adjudicate on the architecture and design choices of the system, as it was outside the scope of its jurisdiction; instead, it once again reiterated the need for a robust privacy framework to mitigate any privacy risks that the system introduced.[95]

Security of System, and Vulnerability to Hacking and Unauthorised Access

In **Jamaica**, the court was quick to recognise the many dangers associated with the vast collection and storage of personal data. They observed that due to the nonrivalrous nature of data, its misuse and abuse is easy and can often go undetected.[96] Hacking is typically not disclosed by the hacked entity, and once stolen the data is difficult to trace and retrieve.[97] Although they spoke at length about requiring robust and deterrent systems to minimize data theft, the

90 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 224, ¶ 101.

91 Section 17(e), National Identification and Registration Act, 2017.

92 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 56.

93 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 855.

94 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 882.

95 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 875.

96 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 247(A)(80).

97 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 247(A)(79).

court recognised that regardless of protection offered by a strong statute, it is insufficient to comprehensively secure data proposed to be collected and stored, of an entire nation, for generations to come. Thus, the court determined that the threat of hacks and unauthorised access was so severe when the data collected is vast and pervasive, as is in a national digital ID program, that it warranted its complete upheaval.[98] Thus, the threat of unauthorised access was held to put data subjects at the risk of a violation of their privacy.

In **Kenya**, the court observed that the storage of biometric information in the absence of a strong legal framework put data subjects at the risk of "attack or unauthorized access", and therefore impacted their privacy rights.[99] This was enhanced by the centralised storage of such data, since it had the added effect of the data subjects having no information or control over their own data, and often no knowledge of its access.[100]

A chief criticism of the Aadhaar judgment in **India** was how callously the court treated the risk of hacking and unauthorised access of the ID system, despite much evidence of its repeated instances. In spite of referencing several newspaper reports of unauthorised access of the Central Identities Data Repository ("CIDR") — all of which were denied by the UIDAI — the court did not hear parties on the subject[101] and relied on an assurance of the respondent to ensure the security of the CIDR.[102] However perhaps even this small exchange is indicative of the court's fears associated with the risk that unauthorised access imposes on the privacy of data subjects.

98 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 247(A)(123).

99 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 880.

100 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 880.

101 This issue of the court's engagement with technological evidence will be explored in greater detail in a subsequent post in this series.

102 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 212 (Sikri, J.).

Accountability of Administrator

In **Jamaica**, the court held that a lack of provisions for auditing the Authority, or otherwise holding it accountable, to see if it is complying with the law, put at risk the privacy of ID holders.[103]

In **Kenya**, the court observed that the Accountability principle, under the OECD privacy Principles,[104] required the data controller to be accountable for complying with measures that enhance privacy.[105] The Data Protection Act, that is applicable to the *Huduma Namba* framework, provides for an independent Data Commissioner to oversee the implementation of the Act. It was held that until all aspects of the Data Protection Act were operationalised, including by codifying circumstances in which the Data Commissioner might exempt the operation of the Act, or by appointing the Data Commissioner and registering data controllers and processors, the lack of accountable administration of the system puts at risk the privacy of data subjects.[106]

Storage of Data

The court in **Jamaica** held in its assessment of the privacy claim, that regardless of whether the Digital ID scheme was voluntary, the storage of the data collected in the scheme itself would run afoul of the constitution, because of the privacy risks it exposes data subjects to.[107]

In **Mauritius**, the retention and storage of the biometric data collected for the issue of the ID card was of particular import to the Supreme Court.[108] The NIC Act provides that a register will record all the data collected of every citizen,[109] and will include other "*reasonable or necessary information as may be prescribed.*"[110] The court held that the storage and retention of personal information for an indefinite

103 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 247(A)(82).

104 "OECD Privacy Principles", Organisation for Economic Co-operation and Development, last accessed June 9, 2020, *http://oecdprivacy.org/*.

105 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 850.

106 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶¶ 852-853.

107 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 247(A)(51).

108 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 28.

109 Section 3(1), National Identity Card Act, 1985.

110 Section 3(2)(b), National Identity Card Act, 1985.

period violates citizens' fundamental right to privacy, and is a disproportionate action to be exempted as a "justifiable" aim to pursue.[111]

In **Kenya**, the court observed that the centralized storage of biometric data subjects ID holders to unauthorized access or attacks, perhaps without even their knowledge, entailing irreversible risks of misuse of the data for discrimination, profiling, surveillance, etc.[112] They concluded that this is the nature of all biometric systems, whether centralised or not, and therefore required a secure legal framework with detailed regulations and procedures, all of which the current legal framework did not satisfy.[113] Thus, the storage of biometric information, particularly in the absence of a sufficient legal framework, threatened the privacy rights of individuals.

Amount of Data Collected

In **India**, a crucial concern of the petitioners in the Aadhaar case was that the all-encompassing data collected and stored in the Aadhaar framework enabled a "cradle to grave" surveillance State, that could easily be abused by an unscrupulous government/private actor.[114] To determine this, the court tasked itself with answering two questions: first, whether the Aadhaar project enabled the government to have enough data to profile data subjects; and second, whether there were enough safeguards in the governing framework to preclude this.[115] Although purporting to answer the first question, the court primarily discussed how the Aadhaar architecture attempted sufficiently to minimise data leaks in the process of collecting information. Its only observation on the issue of the amount of data collected was that on every use of Aadhaar for authentication, the only data being disclosed and/or recorded is the "yes" or "no" response, along with the Aadhaar number and the requesting entity's identity. The Authority would only be privy to information about the identity of the Aadhaar User Agency, and the device used for authentication, without any information about the location of the transaction, the IP address, its operator, the purpose of authentication, etc.[116] They concluded that it would be difficult to profile a data subject based merely on the

111 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177 30, 34.

112 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 880.

113 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 884.

114 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 130.

115 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 150.

116 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶¶ 151-152.

basis of their biometric and demographic information stored in the CIDR, and to that extent there was no privacy risk caused by the amount of data collected for Aadhaar.[117]

Authentication of ID

In **Jamaica**, the NIRA has not yet operationalised the authentication mechanism for the use of the Digital ID, and to that extent does not have a governance framework for authentication. Accordingly, it does not in any manner prevent the Authority from storing data regarding the purpose for which the requesting entity is seeking authentication. The storing of metadata, apart from that regarding authentication transactions, is also not expressly prohibited. The court, justifiably concerned about the implications of all these failures, registered its fears about the use of Digital IDs for authentication purposes.

In **India**, a key privacy concern of the petitioners in the Aadhaar litigation was that of the data collected at every authentication of the Digital ID. Since a primary mode of authentication was by using fingerprints, data subjects were parting with their biometric data at every use of Aadhaar, and with several different actors (who are permitted to leverage the Aadhaar authentication mechanism). Keeping records of every authentication also facilitates a monitoring of the transactions of the data subject in manner that resembles real-time surveillance, and could therefore easily be misused. However, the court held that while such concerns exist in principle, the Aadhaar framework has effectively eliminated such an occurrence.[118] The Aadhaar Act and its adjoining regulations prohibit the authority from collecting and storing any information about the purpose of the authentication.[119] Even data concerning the location is not determinable by the authority.[120] "Authentication record" is defined to mean a record of the identity of the RE, the time of authentication, and the response provided by the authority.[121] The device used for authentication is only equipped to recognise the identity of the RE, the PID, the code of the device, and the time and nature of response.[122]

117 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 153.

118 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 297 (Sikri, J.).

119 Section 32(3), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; Regulation 26, Aadhaar (Authentication) Regulations, 2016.

120 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 197 (Sikri, J.).

121 Section 2(d), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

122 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 197 (Sikri, J).

However, the court held that a maintenance of authentication records for 7 years (as is required by the Act) was unconstitutional as it was an unjustifiable impairment on the privacy rights of data subjects.[123] The court also looked at the meta data collected on every authentication transaction. Metadata was permitted to be recorded by the Aadhaar Act, without limitation as to its category. The court held that allowing all categories of metadata, including data about the location of a transaction, the IP address of the transactor etc would sanction the disclosure of an individual's personal data and impact their privacy rights.[124] Thus, while the court did recognise in principle the harm that can arise to an ID holder's privacy rights from the use of an ID for authentication, it held that the legal framework governing Aadhaar sufficiently proscribed it.

In conclusion, the issue of privacy formed the crux of the petitioners arguments in all the cases, and took the most attention of the court. All the courts seemed to recognise the integrated privacy impacts of a digital ID system, but there were some factors that distinguished their ultimate decisions. In India, privacy rights were not accorded to all information, but only the information that had reasonable expectation of privacy; factors that were considered here were whether the information was already in the public domain, whether it would be injurious to the individual if such information was disclosed, etc. This diluted the petitioners claims for the protection of biographical and demographic information. Kenya had similar considerations of "reasonable expectation of privacy" for private information, but categorically held that this would encompass any information that an individual did not want to share, even regarding their actions in the public sphere. Eventually they adopted the definition in their Data Protection Act, which mirrored that of the GDPR, and found any identifiable information about a person to be "private information" warranting protection. Similarly in Jamaica, all information was considered private, as the determining factor of privacy was the control it gave to an individual over their data. Thus, the Indian court's approach in the Aadhaar case pivoted, to some extent, on its treatment of "private information" that deserved protection. Since the Mauritius court only considered bodily privacy, it did not rule on the nature of information that is protected under a right to privacy. There was also an important disparity in the idea of consent and coercion in the collection of biometric data. The judges in Jamaica held that it was the lack of consent in collection of biometric data (because of the criminal sanction in place for failure) that violated their fundamental right against unreasonable searches and for their private life to be respected. The legal and design framework surrounding the digital ID program

123 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 199 (Sikri, J.).

124 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 201 (Sikri, J.).

was still to be examined for privacy violations however, *even* if the data was shared with consent. This is because any further unconsented disclosures of data hinges on the system that stores and protects it. However, in Kenya, despite the court recognising that a majority of the more recent registrations for NIIMS was done consensually, it had to still be examined for its potential privacy implications, particularly because the petitioners challenged the relevance of biometric data (and their privacy right protects Kenyans from "unnecessary" sharing of personal information). This was also missing in the judgment in the Indian Aadhaar case, as the court only addressed the privacy implications of those parts of the governing Act that made Aadhaar mandatory. Although the Kenyan jurisprudence can be attributed to the wording of their privacy law, it still forms an important observation because it identifies that sometimes consent, particularly when the actors in question are an individual and its State, is not a sufficient factor to protect individuals' privacy.

However, what must also be noted is that it was largely only in the Aadhaar case that the protection of non-biometric data was also sought by the petitioners; in all the other cases, it was primarily core biometric information that was contested. With the exception of India, authentication information did not form a part of the petitioners cases even though it is a major privacy concern. This is possibly because the authentication mechanisms and the uses of the ID system had not yet been properly determined in these countries.

Another concerning issue that was treated radically inconsistently was that of the linking of databases through a unique ID. While Jamaica was quick to understand all the risks that came with such linking, the Indian court easily permitted it for some purposes that were even outside the purview of the Aadhaar Act. The Kenyan court, in a trend that would continue for several other important determinations, refrained from ruling on the "design and architecture" of the system. This even when the NIIMS system envisioned the integration of *all* government databases. This did not come up as an issue in Mauritius, as the ID system has not yet envisioned linking of databases.

SECTION II. SURVEILLANCE

The court in **Jamaica** saw the mass storage of identity information, including biometric information, of all its residents in the NCID as enabling surveillance. The embedding of residents' registration numbers, together with the linking of all government databases through this number, made tracking of resident behaviour easy.[125] They recognise that although this may not be the intention of the government, it is a possibility created solely by the NIRA legislation, and this risk alone warrants careful consideration. J. Sykes' observed that "*History has taught us that once the power is available and there is no constraint, governments will use that power.*"[126]

One of the grounds on which the court eventually struck down NIRA was that it did not adequately prevent the use of data obtained from the program for the creation of profiles, and eventually for the creation of a "Surveillance State."[127] The broad scope allowed for information sharing and verification, along with the use of the system for identity verification by the public and private sector with little control, contributes to the creation of easy surveillance by the State.[128]

The court in **Kenya** largely looked at surveillance on the basis of the GPS information that the *Huduma Namba* scheme sought from ID applicants. It held that GPS coordinates are satellite based, and with information taken from providers of internet and telecommunication services, real time tracking of people without their knowledge can be undertaken.[129] Accordingly, without appropriate measures in the legal framework to prevent misuse of GPS information, it cannot be collected.[130] The court also briefly recognised the risk of surveillance fostered by the use and collection of biometric information, which are uniquely and *permanently* linked to individuals, and the centralized storage of such information.[131] Once again, however, it held that such risk can be mitigated

125 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 30.

126 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 30.

127 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 375.

128 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 375.

129 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 768.

130 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 771-773.

131 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 880.

by having in place a secure and robust governing framework.[132] Although the petitioners made many arguments on the risks NIIMS introduces to allowing easy surveillance of the Kenyan population, the court did not address such concerns adequately, and in fact even held that there was no requirement of a purpose limitation to the program since the only "purpose" of NIIMS was for *identification* of the user.[133]

In **India**, when tasked with addressing the claim of whether the Aadhaar program enhanced the powers of the State to engage in surveillance, the court set out to determine two things: first, whether the architecture of the Aadhaar scheme — and more specifically the information assimilated — allowed surveillance and tracking; and second, whether the surrounding legal framework allowed it. The petitioners argued that the project creates architecture suitable for a "cradle to grave" surveillance State and society.[134] The use of Aadhaar for authenticating transactions enables the State to profile users, track movements, assess their habits, and influence their behaviour.[135] Overtime, this can even be used for more perilous intents such as to stifle political dissent. They argued that authentication records, stored in the CIDR, comprise transaction data that enables the State to track the location of the ID holder seeking authentication as well as know the activity they are engaging in. Authentication records include time of the authentication and identity of the requesting entity (with whom the individual is transacting), and can be stored for upto 7 years.[136] Along with other information that the Authority has- such as the user's Aadhaar number, their name, the authentication response (whether authentication was successful), reason for failure of authentication, requesting entity's IP address, device ID and unique ID of authentication device.[137] This concentration of information in one Authority puts the State in a powerful position and its citizens in a compromising one.

The respondents claimed that minimal information was collected from applicants, most of which was already in the public domain.[138]

132 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶¶ 883-884.

133 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 786.

134 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 219, ¶ 130.

135 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 219, ¶ 130.

136 Regulations 20, 26-27, Aadhaar (Authentication) Regulations, 2016.

137 "Aadhaar Registered Devices – Technical Specification – Version 2.0", Unique Identification Authority of India, last accessed June 9, 2020, *https://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_09112016.pdf*; *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 131.

138 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 232, ¶ 144.

Sensitive information that can be used to profile and discriminate against persons, such as race, religion, caste information, was specifically excluded.[139] It was argued that surveillance, if at all possible, could only be carried out by unauthorised use of CIDR information, and would amount to illegal surveillance.[140] However, this would not be a case of the Aadhaar architecture allowing surveillance, and should not be accounted for while determining its constitutionality.

Addressing the first part of its question, the court held that minimal biometric and demographic data is collected during enrolment, and no information about the location, purpose, or other details about the authentication transaction is taken. Sufficient safety precautions are taken in the authentication process, with only "yes" or "no" responses being permitted, and limited exposure of this process to the internet. Further, the enrolment and authentication processes are strongly regulated, with constant oversight and a secure chain of communication with actors appointed/controlled by the Authority.[141] They held that while the Authority does get the unique device code used for authentication, it gets no information related to IP address or GPS location where authentication is completed, and therefore does not know the location or purpose of the transaction.[142] Thus, on the basis of this, it was concluded that it is very difficult to create a profile of a person only on the basis of the information found in the CIDR, and since authentication information was both insufficient and securely protected, it could not be used to track/surveil citizens either. As for the assessment of whether the surrounding legal framework sufficiently guarded against the creation of a surveillance State, the court struck down some concerning provisions, and dismissed the claim of an Aadhaar surveillance State.[143]

Though inherently enhanced by the very existence of a national digital ID program, the risk of surveillance was quite easily dismissed by courts. Some factors of an ID system that increase the surveillance capability of a State are: lack of a legal limitation on uses of the ID system; inadequate oversight by an independent body; the collections of wide varieties of data; the use of a unique

139 Section 2(k), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

140 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 234, ¶ 147.

141 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 236, ¶ 151.

142 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 242, ¶ 152.

143 These provisions include reducing the period of retention of authentication records, prohibiting the storing of metadata, disallowing the participation of private parties, etc. See *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 301, ¶ 230; 293, ¶ 219.

identifier to integrate different silos of information; and the lack of a data protection law that applies to the State. India, though meeting nearly *all* of these criteria, only put in place some limitations pertaining to the period of storage of authentication information and metadata. The court reposed faith in the government to bring out a data protection law that adequately addresses the remaining concerns, which hasn't yet been actualized nearly two years later. In the absence of this law, India does not have any data protection framework that applies to the government. What such a framework would also have ensured is the operation of an independent data protection authority, who would be able to oversee the actions of the administrator of the ID system. Without this, there is no scope of oversight to actualize the measures the Aadhaar court or the ID law implements. The Kenyan court was also dismissive of the danger of surveillance — one that it was certain could be avoided by a rigorous digital ID framework — although it refused to allow the project to continue until all aspects of its governance were properly codified and all oversight mechanisms in the data protection law actualised. Nonetheless, the integration of the national database with all functional government databases as envisioned by the program — thereby linking various categories of information about individual ID holders — is a precursor to State surveillance. Only Jamaica considered this issue as it deserved, and held that merely the existence of so much data with the State created the possibility of pervasive surveillance that could not be ignored.

SECTION III. IMPACT ON CHANGING CITIZEN-STATE RELATIONS

The position of a citizen qua the State is often cemented by the Constitution of a country, and the power it allows the State to have over individual citizens. The existence of a national digital ID program has the potential to fundamentally alter this: by collecting vast biometric and demographic information on a national scale; making it easily accessible through a unique ID; and by tracking the transactions an ID holder does using the ID, the State is now equipped with enough information to change this power balance.

In **India**, the Aadhaar project was challenged on this ground in K.S Puttaswamy v. UOI, and Binoy Viswam v. UOI.[144] Petitioners argued that a fundamental feature of the Constitution is the sovereignty of the people with limited government authority.[145] "Limited government" is integrated into the Constitution in many ways: by the distribution of power among State organs and checks on the exercise of such power; by Fundamental Rights that limit the encroachment of State into the liberty of citizens; by the Preamble to the Constitution, that entitles citizens to live without being under the constant gaze of the State; by the interplay of Fundamental Rights and Directive Principles of State Policy, etc. Attempting to find respite in principles of Constitutional Trust and constitutional morality, they argued that although not codified as such, the requirement of a "limited government" has always been a key feature and goal of the Constitution of India. The Aadhaar project threatens to completely overhaul this, with the State dominating its citizens, for the following reasons:

a. Routine activities such as opening a bank account, receiving government pension, operating a mobile phone, etc can no longer be performed by a resident without the State knowing about it.

b. With information available at hand, the State can easily profile individuals and keep track of their behaviour.

c. Because of how widely Aadhaar is being used as proof of the identity of individuals, the State can cause their civil death by simply disabling their Aadhaar ID.

144 *Binoy Viswam v. Union of India*, 7 SCC 59 (2017).

145 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 374.

d. The pervasiveness of Aadhaar, and therefore the State, limits the personal autonomy of individuals.

e. Where otherwise accountability and transparency is being demanded by citizens from the State, in the case of Aadhaar this is being entirely overturned and extreme transparency in a citizen's everyday life is being demanded by the State.

The court, on its part, agreed with this argument in principle. It held that the Supreme Court's interpretation of Constitutionalism has always been that there is no room for anarchy or absolutism.[146] However, it disagreed on two main counts:

a. Principles of limited government applicable to democratically elected government are part of the Constitution in the form of delineation of powers of each wing of the government, oversight by the Judiciary, constitutionally allotted responsibilities for the Federal and State governments.[147] The claim that this principle also proscribes the State from collecting and storing Aadhaar data such that it might put the State in a dominant position, does not squarely fall within this. However, the court did not address this in enough detail so as to discern whether or not they disputed this understanding of "limited constitution".

b. As to the factual aspects of the Aadhaar project, the court disagreed with the claim that it threatened constitutional trust and morality. They held that with the legal framework that will now govern the project, after some provisions were amended or read down, there is no danger of creating a surveillance State or otherwise harming the autonomy of individuals.[148]

In its assessment, this court did not give due attention to the idea that merely the existence of such information with the State — even if it does not actively engage in surveillance — creates a chilling effect on the speech and behaviour of its citizens, which in turn fundamentally alters Citizen-State relations.

In **Jamaica**, the court recognised the dominant effect the accumulation of such data would have, without this argument explicitly being brought by the plaintiffs. It observed that the collection of biometric and biographic information of the entire citizenry, together with the use of technology and automation, put

146 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 384; *Manoj Narula v. Union of India* 9 SCC 1 (2014); Govt. of NCT of Delhi v. Union of India SCC Online SC 661 (2018).

147 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 386; *Binoy Viswam v. Union of India*, 7 SCC 59 (2017), ¶ 85.

148 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 388.

great powers over the lives of persons in the hands of the possessors of such data, particularly when it is already powerful actors like the State.[149] The use of a unique ID across different databases only increases the possibility of profiling of data subjects, and when combined with the use of an algorithm to analyse the data, can generate new information about them.[150] As a result, there is a lot more power accumulated with the State.

However, NIRA's effect on the change in citizen-State relations did not play a bigger role in the court's final assessment of the claim, as the operative part of the judgment failed to address whether this would be unconstitutional, and focused entirely on its effect on privacy and surveillance. Nonetheless, this court's recognition of the power that such a pervasive digital ID program gives a State, and its impact on creating a chilling effect on its citizens, was heartening.

This was not recognised as an issue in **Kenya** and **Mauritius**, neither by the petitioners nor by the court.

149 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 237.

150 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 190 ¶ 20.

SECTION IV. IMPACT ON DISCRIMINATION AND EXCLUSION

In **Jamaica**, the primary argument on NIRA's discriminatory impact was that by requiring only Jamaican residents to enrol into NIRA and possess the ID to access the same goods and services that non-residents are accessing, their right to equality under Section 13(3)(g) was being violated. Only Residents are required to enrol (at the risk of criminal sanction)[151] and to mandatorily produce their ID while accessing goods and services provided by public bodies,[152] effectively putting them at risk of being treated unfavourably qua foreigners. Put another way, Jamaican residents had to undergo a rigorous identification process (including parting with biographical and biometric information) while non-residents had no identical requirement to access the same goods/services. The court observed that if the purpose of the requirement of NIN while accessing goods and services of a public body is to verify their identity, there is no rational reason to exclude all other forms of identification, and no justification why the same is not applicable to foreigners.[153] Accordingly, the court held that Section 20, that mandates enrolment from Jamaican nationals, is unconstitutional because it has the effect of putting Jamaican residents in a worse position to their foreign counterparts when accessing the same goods and services from the same government entities. Since no reasonable justification has been tendered for this discriminatory impact, it is to be struck down.[154]

No claims were made about the exclusionary impacts of the use of the ID for authentication, and thus there were no discussions about it.

In **Kenya**, the argument for the exclusionary impact of NIIMS took two main forms:

a. The process of registering for the *Huduma Namba* resulted in discrimination against the Nubian (and other marginalised) communities.

b. The mandatory nature of NIIMS, to access goods/services that Kenyan nationals are otherwise entitled to, results in exclusion.

151 Section 20, National Identification and Registration Act, 2017.

152 Section 41, National Identification and Registration Act, 2017.

153 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 179, ¶ 16.

154 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, 179, ¶ 20.

Article 27 of the Kenyan Constitution guarantees every person to "equality before the law and equal protection and benefit of the law," [155] and proscribes the State from discriminating against any person on any ground including race, ethnic or social origin, colour, etc.[156]

The first question the court addressed was whether the NIIMS law in any way differentiated between members of the Nubian community (and other marginalised groups) and other Kenyans. It was argued that while the law itself does not make this distinction, the effect of the law is different for Nubian members qua other Kenyans: the challenges that the former encounters in acquiring the required identity documents and complete the vetting process to establish their Kenyan nationality is cumbersome and results in discrimination. It is not the NIIMS Act in question that requires any vetting process, but the laws under which identity documents (that are required to register with NIIMS) are issued. Under these laws, there is a requirement to vet persons coming from border communities, which includes Nubians. However, the court held that since the legislation being considered is not the one that differentiates between Nubians and other Kenyans, there can be no determination of unconstitutionality. The only thing the NIIMS act does is introduce a system of registration into the national population register that requires, as one of many qualifications, that applicants should have certain identification documents issued under other Statutes.[157]

As for the exclusionary impact of NIIMS, the court recognised that some Kenyans may face the impact of not having identity documents or having poor biometric data, etc, and to address that, asked for there to be clearly identified a regulatory framework to deal with exclusion. However, it did not find that the possibility of exclusion was sufficient reason to find NIIMS unconstitutional.[158]

In the Aadhaar case in **India**, Section 7 of the Aadhaar Act was challenged for its exclusionary effect on individuals. Section 7 allowed authentication of identity by Aadhaar to be made mandatory to access government "subsidies, benefits, or services." [159] The petitioners argued that since biometrics are inherently probabilistic in nature, using it as a process for authentication will undeniably result in exclusion of genuine persons.[160] Accuracy cannot be guaranteed

155 Article 27, The Constitution of Kenya, 2010.

156 Article 27, The Constitution of Kenya, 2010.

157 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 995.

158 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 1012.

159 Section 7, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

160 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 314.

in biometric technology, and combined with the likelihood of fingerprints (the primary mode of authentication) wearing out or changing with age, or being impacted by accidents, there is a possibility of failure in authentication ultimately leading to exclusion. Even where the projected accuracy of biometric authentication technology is 99.76%,[161] that amounts to about 27.60 lakh individuals excluded in India. Several studies were referred to by the petitioners, to highlight the real-life incidents of exclusion in India by the use of Aadhaar.

The court recognised that such incidents could occur during the implementation of Aadhaar, which is a "work in progress",[162] but refused to acknowledge the studies highlighted claiming they were "disputed questions of fact" whose credence could not be tested.[163] It held that the larger goal of the project was to ensure that the fruits of welfare schemes reached its deserving beneficiaries; thus when it was benefitting millions of Indians, it cannot be invalidated on the mere possibility of the exclusion of *some*.[164] In their assessment allowing the exclusion of 99.76% of the population by reverting to a pre- Aadhaar stage is considerably worse than allowing 0.232% to be excluded with Aadhaar. This was based on evidence by the Respondents that prior to linking the Aadhaar scheme with public distribution services, widespread identity frauds pervaded the system and prevented deserving beneficiaries from accessing public services. Incidentally, while relying heavily on this evidence, the court refused to hear evidence from the Petitioners on the current exclusionary impact of making Aadhaar mandatory.

The court noted that these exclusions could be remedied, and that the government is making sincere efforts to that end.[165] Relying on a circular issued by the UIDAI that allowed individuals to establish their identity by other means in case of authentication failures, the court held that suitable provisions for allowing alternate means of authentication should be included into the governing regulations.[166] The court also held that the terms "benefits" and "services" in Section 7 can only be those that resemble subsidies and welfare schemes, and cannot include other aspects of entitlements, education, etc.[167]

161 As was claimed by the UIDAI in the proceedings of the case.

162 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 316.

163 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 317

164 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 318.

165 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 318.

166 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 319.

167 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 322.

It is notable that the court did not hinge the constitutionality of Section 7 on the inclusion of alternate means of identification; it merely stated that "*it would be appropriate if a suitable provision be made...*" and took "*on record*" the statement of the Attorney General that deserving persons would not be denied benefits due to failure of authentication.[168]

168 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶¶ 447(l)(i)-(ii).

SECTION V. THE PURPOSE OF A DIGITAL ID PROGRAM

A key focus of discussions surrounding Digital ID programs are its intended purpose — in the absence of a stated and specific *purpose*, the ID program serves simply as a central registry that can be used for verifying the identity of individuals. This is dangerous for many reasons, not least because there is no delineated scope of use in such a case, and can be leveraged by actors for purposes not intended or foreseen by those subject to it.

In **India**, this issue came into the limelight when the Income Tax Act was amended to mandate the linking of individuals' Aadhaar number with their income tax returns (and their Permanent Account Number). The Aadhaar ID was intended simply as a means to access subsidies and benefits (evinced by the long title of the Act itself), and therefore allowing this additional use was challenged before this court in two cases.[169] An additional concern is the manner in which this use was brought about: the Aadhaar Act was not amended to reflect this change, but an entirely different legislation was modified to use the Aadhaar ID. This effectively eliminates any purpose limitation instituted in the Aadhaar Act itself. Notably, while the Aadhaar Act (and the judgment) make possession of Aadhaar ID voluntary — except to avail benefits/services under Section 7 — the Income Tax Act amendment makes it mandatory for all tax paying citizens.

This court held similarly in both cases. They found that there was no conflict between the Aadhaar Act and the amended Income Tax Act as "*when interpreted harmoniously, they operate in distinct fields.*"[170] The majority measured the amendment for its violation of individuals' fundamental rights using the proportionality test,[171] and on finding that protection of the interests of revenue was a legitimate interest of the State, held that the seeding of Aadhaar numbers to ensure deduplication and eliminate fraud passed the proportionality test. On the issue of the IT Act making mandatory what the Aadhaar Act didn't, the court held that since this was not a case of a parent legislation and subsidiary legislation, the court will not question "*the prerogative of the Parliament in making*

169 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019); *Binoy Viswam v. Union of India*, 7 SCC 59 (2017).

170 *Binoy Viswam v. Union of India*, 7 SCC 59 (2017), ¶ 136.2.

171 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 503, ¶ 425.

a provision directory in one statute and mandatory in another." [172] This is contrary to J. Chadrachud's dissent, where he recognised that the Aadhaar Act, by establishing the Aadhaar system, functions as a parent legislation to any other legislation that were to leverage the Aadhaar system.[173] As a result, therefore, of the majority's opinion, the governance established by the Aadhaar Act is diluted, as it has limited efficacy on uses of the Aadhaar system endorsed by any other law in India. To put into perspective, this means that the entire process of obtaining an Aadhaar ID, along with the risks involved in storing it, and the privacy harms arising from allowing disclosures and third party access, can be made mandatory for a purpose not even envisioned by the Aadhaar Act.

In **Kenya**, the issue of a purpose limitation to the ID project was brought up in court, during the assessment of whether information taken under the ID law was "necessary" for its stated purpose. It was argued that the project itself was "purpose free," and therefore it could not be shown the extraction of biometrics was necessary for the goal of the project.[174] The court, on assessing provisions of the NIIMS Act, held that NIIMS is primarily an identification and verification system. Its purpose is to create a national population register, assign unique IDs, and verify and authenticate identities of persons.[175] For this, it is necessary to have a database with biometric data, for comparison.[176] In this way, the court held that the purpose of NIIMS, of creating an identification system that would serve as a "single source of truth", was in public interest, and therefore constitutional.[177] This is also reflected in the case of the Respondents, when they stated that NIIMS was established to help the State secure protection of national security, prevention and investigation of crime, provision and delivery of national services, etc.[178] Thus, there was no particular purpose of NIIMS other than simply to verify the identity of those resident in Kenya.

In **Jamaica**, the Robinson case does not address the issue of assigning a purpose to the ID system, beyond that of verification of identity. A study of the NIRA reveals that its goal or purpose is simply to establish a registry — the National Civil and Identification Database — to issue a National Identification Number (NIN), National Identification Cards (NIC), etc. All of this points to an end purpose simply of identification. This is seconded by the judges' own understanding of NIRA,

172 *Binoy Viswam v. Union of India*, 7 SCC 59 (2017), ¶ 92.

173 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶ 278 (Dissent, Chandrachud, J).

174 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 774.

175 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya). ¶ 786.

176 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 787.

177 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 790.

178 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 411.

as a "system of data collection on all Jamaican citizens and those who live here for at least six months."[179] The Act mandates public bodies to require the NIN or NIC for their delivery of goods or services, and allows private entities to do the same, never restricting the nature of goods/services this is applicable to.[180] Even the Attorney General, representing the Respondents, claimed that the purpose for enacting NIRA was that Jamaica lacks a reliable national identification database.[181] The existing identification system does not allow data sharing and is not interoperative, and thus allows the creation of multiple identities.[182] This was something the court vaguely recognised while determining whether NIRA was a proportionate measure, as a key point of differentiation from the Aadhaar system — which was targeted at social welfare delivery[183] — and held that *if* social welfare was the goal, then the Act constitutes overreach.[184] In this manner, there is no purpose limitation ascribed to NIRA either through the Act or the judgment.

In **Mauritius**, the ID case was prompted by the national identity card being replaced by a new biometric card. The National Identity Card (Miscellaneous Provisions) Act only largely dealt with the mandate and process of registration for the Card, and did not address any uses ascribed to it. Even while analysing the legal framework surrounding the Digital ID, the court was assessing the Data Protection Act and its applicability to the ID project, which understandably was not tailored to the ID project itself. Thus, the project did not come with an intended use or purpose, but was simply to function as an identity card for any situation that may require a verification of identity. The court analysed the intention of the Act as that of "establishing a sound and secure identity protection system" to protect against identity fraud, and held it to constitute a legitimate purpose.[185]

179 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 29.

180 Section 41, National Identification and Registration Act, 2017.

181 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 309.

182 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 309.

183 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 335.

184 *Julian J. Robinson v. The Attorney General of Jamaica*, [2019] JMFC Full 04, ¶ 355.

185 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 28.

CONCLUSION AND OBSERVATIONS

There were several similarities and differences in how the courts looked at these Digital ID programs, and what led to their ultimate decisions.

Where the privacy issues lay:

Broadly, the courts' assessment of the violation of privacy rights by the national ID project can be divided into three parts:

a. Privacy impacted by the collection of biometric and demographic information at the stage of identification,

b. Privacy impacted by the collection and recording of authentication data, and

c. Privacy impacted by an inadequate legal framework (since the courts refrained from commenting on the design framework/architecture) that allowed further disclosures of information.

While nearly equal concern was assigned to the first and last points, all the instances of shutting down or temporarily stalling the project was because of the inadequate legal framework. Thus, the collection of vast amounts of information from citizens was not considered to pose sufficient threat to users' constitutional rights. In the court's consideration, the existence of an intrusive and integrated Digital ID system, that potentially impacted the power States had over its citizens, was not unconstitutional so long as there was a legal framework that sufficiently controlled this power. More concerning was possibly the dismissal of the threat caused by the recording of authentication logs, facilitating the creation of a surveillance State. Although a major concern in the Aadhaar case in India, it was merely identified by the court in Jamaica — without forming a substantial part of its order — and was entirely ignored in Kenya and Mauritius. Even the aspect of consent in the collection of data was treated differently by different courts: in India, Jamaica, and Mauritius, it was only the mandatory parting with personal information that was considered for its privacy implications. In Kenya, the court acknowledged that persons were not being coerced to part with their personal information, and assessed the privacy impacts of collection of this data on other grounds. Perhaps in the case of Jamaica and Mauritius the courts had no reason to assess the impact of collection of data with consent, but in India, where most of the uses of Aadhaar were voluntary, the court had the opportunity to assess privacy implications of the collection of such data even *with* consent. However, they restricted their assessment to sections 7 and 8 of the Aadhaar Act, which made the possession of Aadhaar mandatory.

A Constitutional Right to Privacy

The scope of the privacy violation caused by the ID system was impacted by the existence and nature of a constitutional right to privacy. In Kenya, it was only considered a threat to the privacy of residents if the data collected by the project was "unnecessary" for its purpose. This stemmed directly from its constitutional protection of privacy, which had been codified rather narrowly. Similarly in Mauritius, the court only assessed the likelihood of the biometric ID card impacting citizens' constitutional protection of bodily intrusion. By refusing to interpret their right to privacy broadly, the Mauritius court eliminated any constitutional right to informational privacy for citizens. India, on the other hand, began to conceive a fundamental right to privacy only in the context of the Aadhaar program, and therefore the right that was born was broad enough to cover most acts of the ID project. The right to privacy was found in the rights to life, liberty, freedom, and dignity, and therefore encompassed a whole set of connotations going far beyond a typical meaning of privacy. Amongst other things, this right is up to date in the technology-driven world we now live in, which we perhaps cannot say so easily about several other constitutional protections predating this one. Jamaica, the only exception to this pattern, had a narrow constitutional right to privacy but chose to use its constitutional rights to freedom, liberty, and dignity, to check the intrusive features of their ID card project that otherwise escaped their privacy rights.

Engagement with the Exclusionary Effects of National ID Schemes

The potential of national ID schemes to exclude entitled users from accessing services and benefits was a key concern in the pushback against their implementation. However, engagement on this issue by the courts was dismal; in Jamaica and Mauritius, the petitioners failed to sufficiently challenge this aspect in their case; in Kenya and India, although it formed a substantial part of the claims, the courts reposed trust in the government to protect users from exclusion, without requiring any actions or halting the project on the contingency of the fulfilment of the government's guarantee. In India, where the use of Aadhaar for accessing important government services is already in play, it was a particularly dangerous outcome. The court also arrived at its decision in a questionable manner; it pit an individual's right to privacy against their right to food, which it assumed was *only* obtainable by having the Aadhaar identification system be linked with public distribution schemes. By doing this, it was able to hold that the absence of the Aadhaar scheme would have a far wider exclusionary

effect than any similar impact the presence of Aadhaar would. This is curious, as the contention in question was not merely the existence of the Aadhaar scheme, but the act of making Aadhaar authentication mandatory to access public services. The court failed to show why it would need to be mandatory, when it was a question of an individual's right to food versus their right to privacy, as ideally the individual must be permitted to choose what they would prioritise (if it was a trade-off at all).

Stage of Implementation of Project

A key factor important to the outcome of these cases is the stage of implementation of the projects when ultimately decreed by the courts. The Jamaican project, NIRA, was created in December 2017 but hadn't yet been brought into force when the court decided the matter in 2019. The NIC Act in Mauritius was passed in July 2013, and implementation began in October 2013; the project was less than 2 years old when the court ultimately decided its constitutionality in 2015. In Kenya, operation of *Huduma Namba* began only in 2019, when the court decided the case in early 2020, with timely interventions during the hearings in the form of injunctions to the government. In India however, Aadhaar was being discussed as early as 2006, and its operationalization began in 2009, with the Aadhaar case only being decided in late 2018. In its judgment, the bench insinuated several times that it could not "shelve" a project that already had scores of enrolees and beneficiaries, and for which much taxpayer money had already been consumed.[186] Thus, the best route it found was to mitigate damage caused by the project, by reading down or nullifying some of its more treacherous features. This was not a factor that other courts had to take into consideration, since the national ID projects in those jurisdictions were still in its infancy, with minimal damage done and money spent, and few users. Thus, the stage of implementation of the project has played a crucial role in ultimately determining its validity.

186 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), 44, 296 ¶ 220; 387 ¶ 319.

Courts' Engagement with Biometrics

In all of these cases, a key point of point of issue was the use of biometrics in the deployment of a national ID program. There were largely two ways in which the use of biometrics was challenged: first, in the risk they posed to the privacy of ID holders; second, in their utility and suitability as identity authentication technology. However, across the cases, the courts insufficiently engaged with the issue, particularly with the second leg. Biometric technology was either taken as a defacto mode of identification, most suitable for the purposes of a national ID scheme, or entirely ignored in the guise of judicial deference. In India, although the petitioners contested the suitability of a technology that produces, at best, probabilistic results, the court refused to engage in an independent assessment of biometric technology. Despite evidence from the petitioners of the false positives and negatives that biometric technology allows, as well as the documented cases of duplication persisting after the process of deduplication by Aadhaar, the court continued to hold the factual assumption that it is only biometric technology that can result in *unique* and reliable identities.[187] Even while assessing the use of biometrics in the proportionality test, for the risks of privacy and unfair exclusions that it introduces, the existence of better and equally effective alternatives was never properly considered by the court. Although largely a technological matter, little technological expertise or evidence was examined. In Jamaica, while studying the nature of biometric systems, the court relied simply on J. Chandrachud's dissent in the Aadhaar judgment. In the Mauritius case, the testimony of the operators of the ID system as to the importance of biometric technology was never challenged (per the court) and the court was convinced of its suitability for the ID project.[188] Only in Kenya was the issue of biometrics given any real consideration: the court heard expert witnesses on the nature of biometric technology, and deliberated its applicability to a robust ID system. It described how the permanent and universalistic nature of biometrics made it a suitable technology for identity verification. However, even in its assessment, it failed to engage sufficiently, claiming that issues of the design of an ID system was entirely within the ambit of the executive and did not warrant judicial review.

187 "Take me as I am – subject to Aadhaar-Based Biometric Authentication: An Overview of the Aadhaar Judgement", Indian Constitutional Law and Philosophy (blog post), last accessed June 9, 2020, *https://indconlawphil.wordpress.com/2018/09/26/take-me-as-i-am-subject-to-aadhaar-based-biometric-authentication-an-overview-of-the-aadhaar-judgment/*.

188 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 26-27.

Nature of the ID system

National ID systems have taken widely different identities or forms in the different countries that have introduced them. At this juncture, it is not unwise to ask what unifies them into a category of Digital ID systems, besides their employment of digital identification technology. Digital IDs were touted as solutions for the problems of inaccessibility to government benefits or services because of the ease they introduced to the system, along with their potential to eliminate fraud and duplication. Their ability to facilitate the delivery of these government services was the leading factor behind their deployment in developing countries, as well as for refugees and displaced persons.[189] They were intended to be tools in the hands of individuals, who can use it to establish their identity and access goods or services with minimum friction.

However, what is noticeably happening instead is the creation of a digital database of sorts, with credentials to allow ID holders to also authenticate their identity. This way, while nothing ostensibly changes of the agency or control the ID holder has, the aim of ID systems has changed: from being the means through which a deserving beneficiary can access government goods or services, to being a tool the State can use to allocate an identity to its citizens for reasons of national security, detection of crimes, enforcing public order, etc. We see this directly in the cases of the ID system in Kenya, Jamaica, and Mauritius, and indirectly in India. The State's emphasis on connecting different databases through a seeding of a unique ID, on its potential to help national security and crime detection, and on refusing to allocate a specific purpose to the system, in Kenya, Jamaica, and Mauritius indicate a goal less skewed towards accessing government services. Even in India, where Aadhaar is modelled as a system to better the delivery of subsidies and services, its newly legislated use for detection of fraud in the payment of taxes is indicative of an altered goal, more in line with its aforementioned peers. Similarly, the disclosures allowed in these systems, for reasons of national security, investigation of crimes, etc are not aligned to a focus on providing transactional ease for ID holders.

189 "Identification in the Context of Forced Displacement", Bronwen Manby, World Bank, last accessed June 9, 2020, *http://documents.worldbank.org/curated/en/375811469772770030/Identification-in-the-Context-of- Forced-Displacement-Identification-for-Development-ID4D*; "Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints", World Bank, last accessed June 9, 2020, *http://documents.worldbank.org/curated/en/745871522848339938/Public-Sector-Savings-and-Revenue-from- Identification-Systems-Opportunities-and-Constraints.pdf*; "The Identification for Development (ID4D) Agenda: Its Potential for Empowering Women and Girls", Mariana Dahan and Lucia Hanmer, World Bank, last accessed June 9, 2020, *http://documents.worldbank.org/curated/en/859071468190776482/The-identification-for- development-ID4D-agenda-its-potential-for-empowering-women-and-girls-background-paper*.

Influence of Similar Cases

There is a noticeable difference in how much the courts in question relied on jurisprudence of foreign courts in Digital ID cases. Although there were cases related to privacy and biometrics that were referenced by all the courts, only the influence of national digital ID cases is relayed here, as they deal with unique problems not seen in other privacy cases.

Since the Aadhaar case in India preceded the cases in Jamaica and Kenya, it had only the Mauritian case to guide it. However, the majority made no reference whatsoever to it, and it was only briefly mentioned in the concurring judgment by J. Bhushan [190] for a very limited point [191] On the other hand, the dissenting opinion by J. Chandrachud analysed several cases from other jurisdictions, including the Mauritian case. The Mauritian court, for its part, did not consider the references made by the petitioner to the Aadhaar case, as it held that the Constitution of India was worded differently, and thus the Mauritian Constitution should be interpreted within its own context and framework. [192]

In Kenya, there were several instances of influence by the Aadhaar case: in the definition of informational privacy; [193] in the court's understanding of the limited use of biometrics for authentication of data subjects; [194] and perhaps most importantly in actualization of security standards and safeguards as done in India's extensive set of Aadhaar Regulations, which the Kenyan government had failed to do. [195] Similarly, the influence of the Aadhaar judgment, and particularly J. Chandrachud's dissent, and the Mauritian judgment, is undeniable in Jamaica's judgment. Through an analysis of similar systems and how the judges understood them, these courts were better able to identify and interpret concerns that arise from ID systems. For instance, in the existence of a Data Protection framework, the Kenyan court refused to endorse the validity of the ID system until a proper framework was instituted and operationalized, down to the appointment of a Data Commissioner. This, they claimed, was influenced by the detailed regulations part

190 *Justice K.S. Puttuswamy (Retd.) v. Union of India*, 1 SCC 1 (2019), ¶¶ 193-196 (Bhushan, J.).

191 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177. The Privy Council of Mauritius, on appeal from the Supreme Court, held that the taking of biometric data from the petitioner does not in itself lead to a presumption of criminality, even though it might be used in a criminal investigation. J. Bhushan relied on this point while holding that an apprehension of insecurity of data stored in the CIDR is not grounds for unconstitutionality.

192 *Madhewoo M v. The State of Mauritius*, 2015 SCJ 177, 8-20.

193 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 748.

194 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 777.

195 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶ 884.

of the Aadhaar framework in India.[196] With how much the petitioners attempted to highlight the failings of the Aadhaar system, surely it was similarly influenced by the failure of the Indian government in implementing a data protection law that it promised in court in 2018. In this way, the courts that had the opportunity to and did rely on similar cases from other countries were better able to grasp the harms introduced by a national digital ID program, and insisted on the nuances that could (potentially) mitigate these harms.

196 *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR (Kenya), ¶¶ 884, 885.

APPENDIX A. COMPARISON CHART

COUNTRY	INDIA	JAMAICA	KENYA	MAURITIUS
NAME OF PROJECT	Aadhaar	National Identification and Registration Act, or NIRA	NIIMS or *Huduma Namba*	National Identity Card, or NID
LEGISLATION BEING CHALLENGED & KEY FEATURES	**Aadhaar (Targeted delivery of Financial and other subsidies, benefits, and services) Act, 2016 and other allied regulations; Section 139AA, Income Tax Act 1961; Prevention of Money Laundering (Maintenance of Records) Rules, 2005.** These Acts cumulatively assign unique identity numbers to residents, mandate the authentication of this number to receive certain government services, and require them to be linked to other IDs and bank accounts to prevent tax fraud and money laundering.	**National Identification and Registration Act.** It assigns a unique National Identification Number (NIN) and a National Identification Card (NIC) to every enrolee. The uses of the ID are not yet fully specified.	**Statute Law (Miscellaneous Amendment) Act No. 18 of 2018.** It amends the Registration of Persons Act to establish a national Integrated Identity Management System (NIIMS). NIIMS was to be a single source of personal information, with each individual being assigned a unique number and information being collected/ incorporated from other government agency databases.	**National Identity Card (Miscellaneous Provisions) Act of 2013.** This Act amends the National Identity Card Act 1985, which issues to citizens a national ID, to mandate all citizens of Mauritius to register for a new biometric identity card. All the information collected under this scheme will be kept in a central register by the Registrar of Civil Status.
STATUS (AS OF MAY 2020)	Nearly 90% of the population of India has been enrolled,[1] an authentication mechanism is in play, and Aadhaar is currently being used for a variety of cases.	NIRA was enacted in December 2017, but is yet to be operational.	The Act became operative on 18th January 2019. Enrolments have begun, but uses of the ID have not been formally determined. Post the 2020 judgment, the project has been stalled until a data protection framework had been properly actualized.	The NID Act was passed in July 2013, and its implementation began in October 2013. It was less than 2 years old when the Court passed this order stalling the program.

1 198 "State/UT wise Aadhaar Saturation", Unique Identification Authority of India, last accessed June 9, 2020, *https://uidai.gov.in/images/state-wise-aadhaar-saturation.pdf*.

APPLICABLE TO	All residents of India	All citizens of Jamaica and individuals ordinarily resident in Jamaica	All Kenyan citizens and registered foreigners resident in Kenya	All adult citizens of Mauritius
MANDATORY/VOLUNTARY	Section 7 and 8 of the Act make Aadhaar authentication mandatory for access to certain schemes/ benefits. It is also mandatory for tax payers to link their Aadhaar ID to their Permanent Account Number (that is used to identify persons paying income tax)	Section 20 of the Act mandates every registerable individual to enrol, and has made it a punishable criminal offence to fail to enrol.	Currently, the *Huduma Namba* is not mandatory for access to any government services, but the Huduma Bill 2019 (only a draft, yet to be passed) envisions mandating it to access all public services	The NIC Act allows any person (under reasonable circumstances or when authorized by law) to require the authentication of a citizen by their biometric ID. It also mandates all adult citizens to replace their earlier identity card with this one (and thus, there is a legal obligation to posses this card).
INFORMATION COLLECTED	Demographic information, including name, date of birth, gender, residential address, and biometric data including facial image, all 10 fingerprints, scans of both irises. Mobile number and email address are collected at option of the applicant.	Biographic information including name, date of birth, place of birth, names of parents, gender, height, place of residence, nationality, period of residence in Jamaica (if not citizen), marital status and name of spouse, date and place of marriage, Date of divorce. Enrolees can also share data about their employment status, their race, religion, education, occupation, mobile number, etc on a voluntary basis. Biometric information including photograph, fingerprint, eye colour, manual signature (for non- minors). Optional biometric information includes retina/ iris scan, vein patters, footprint, etc. The database will also include various reference numbers of the enrolee, including their passport number, driver's license number, taxpayer registration number, electoral identification number etc., as well as the registration history of the enrolee.	Demographic information Biometric information (including fingerprints, Hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA), GPS coordinates.	Biometric information including all 10 fingerprints and photograph, and demographic information including name and sex.

TIMELINE OF LITIGATION	The petition contesting Aadhaar was originally filed in 2012, the case was decided in September 2018.	The case began in early 2018 and the final judgment was delivered in 2019.	A petition was filed in February 2019, and the court issued an interim order in April 2019 allowing registration for the ID to continue (until the case is finally settled) provided it was not made mandatory, access to services did not depend on enrolment, DNA and GPS data would not be collected, data would not be shared with third parties, and there was no deadline for enrolment. The High Court passed its final judgment in February of 2020.	Implementation of the project began in October 2013. The Supreme Court of Mauritius decided the case in 2015, and the Privy Council of Mauritius upheld the court's judgment in appeal in 2016.
COURT	Supreme Court of India	Supreme Court of Judicature of Jamaica	High Court of Nairobi	Supreme Court of Mauritius