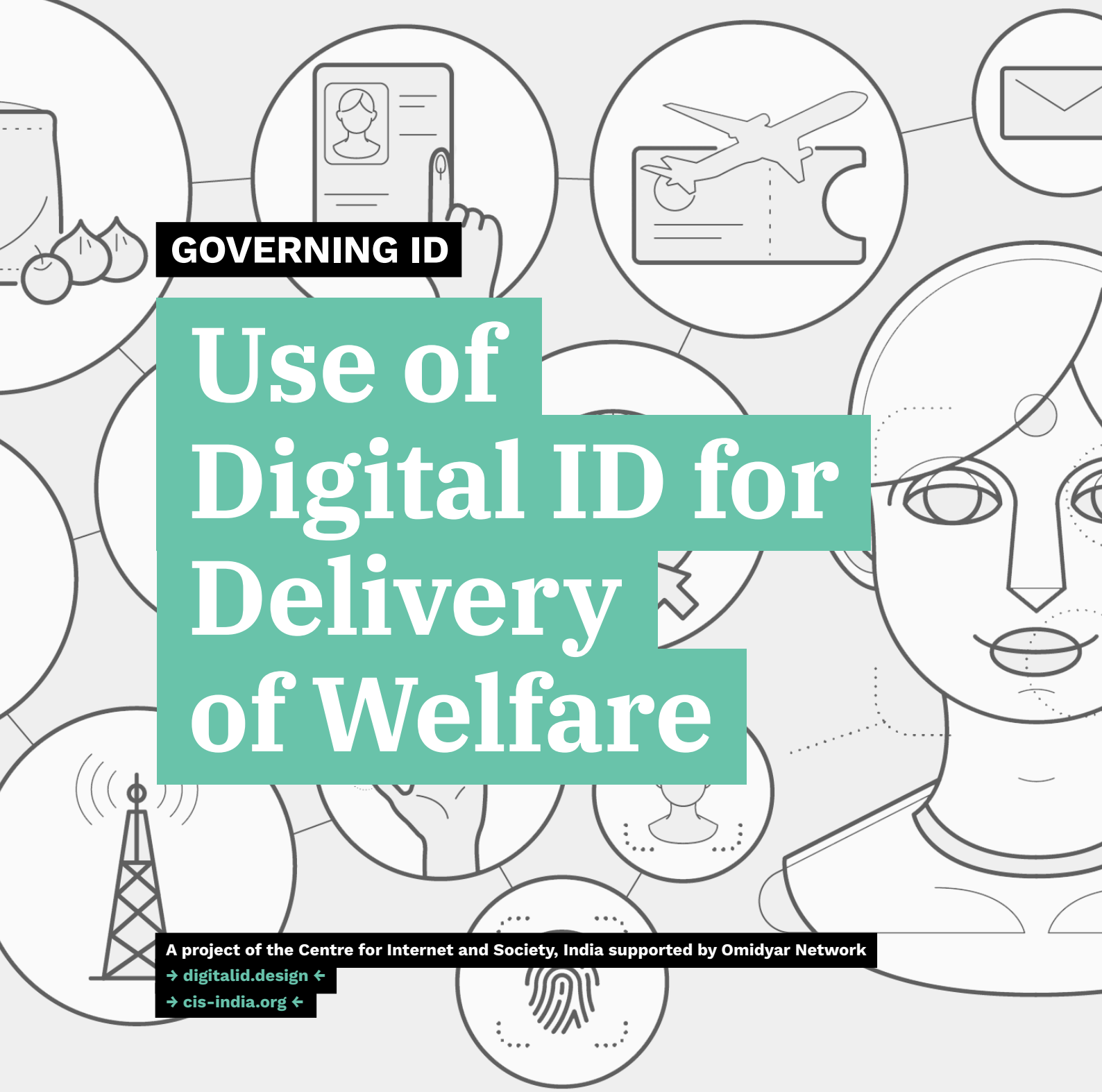

GOVERNING ID

Use of Digital ID for Delivery of Welfare

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

RESEARCH & WRITING
Vrinda Bhandari

REVIEW & EDITING
Shruti Trikanad and Amber Sinha

DESIGN
Pooja Saxena

COVER ILLUSTRATION
Akash Sheshadri

THE CENTRE FOR internet & society

INTRODUCTION

This is the seventh in a series of case studies, using our evaluation framework for the governance of digital identity systems. These case studies, which analyse identity programmes and their uses, illustrate how our evaluation framework may be adapted to study instances of digital identity across different regions and contexts. This case study analyses the use of digital identity in the delivery of welfare by states.

One of the key stated purposes of modern national digital identity systems is to deliver socio-economic welfare benefits by preventing the capture of these benefits. The idea is to ensure that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients.[1] This is attempted to be achieved through the use of Digital ID systems and the process of seeding,[2] authentication, de-duplication and biometric matching. These forms of verification necessarily involve excluding frauds and duplicands from the system. In cases where the digital identity system does not work in the way intended, there are clear exclusionary impacts of such uses, since welfare benefits may be denied to those who are unable to successfully authenticate their digital ID. Below, we evaluate the use of digital identity systems for the purpose of delivery of welfare across jurisdictions.

We are focusing on Kenya, India, and Estonia. The digital ID in Kenya are the Huduma card and the Huduma Namba, that, along with the National Integrated Identity Management System ("NIIMS") database form part of the NIIMS, which operates as a single source of personal identification for citizens and persons resident in Kenya. The Huduma Bill was introduced in July 2019, in the backdrop of petitions challenging the provisions of the Statute Miscellaneous (Amendment) Act of 2018, which amended the Registration of Persons Act to create NIIMS and authorise the collection of DNA and GPS data.[3] The Huduma Bill, 2019 seeks to repeal the Registration of Persons Act. The digital ID in India is the Aadhaar number, which is governed under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 ("Aadhaar Act"). In Estonia, digital identity cards are governed, *inter alia,* by the Identity Documents Act, 2000 and the Population Register Act.

1 *K.S. Puttaswamy v Union of India,* 10 SCC 1 (2017).

2 Seeding is the mapping of identity records in an existing database with those in another database, typically through a unique identifier.

3 "Huduma Namba Bill Analysis", CIPIT Blog, last amended September 26, 2019, *https://blog.cipit.org/2019/09/26/huduma-namba-bill-analysis/*

RULE OF LAW TESTS

1.1 LEGISLATIVE MANDATE

Is the use of digital identity system for provision of welfare codified in valid law?

The first step of our assessment is to evaluate if the law provides for welfare delivery. **In order to be a valid use, the preliminary test is whether the law governing the Digital ID prescribes the use of the digital identity system for welfare delivery.**

In Kenya, the Huduma Bill, 2019 makes it a mandatory obligation to present the Huduma Namba, *inter alia,* to access universal health care services, benefit from the government housing scheme; enrol into a public educational facility; access social protection services; or any other specified services.[4] Every government agency delivering a public service is to be linked to the NIIMS database.[5] Further, the Huduma card serves as the official government issued document for identification (for the aforementioned services) and conduct of transactions.[6] The provision of welfare through the use of the digital ID is thus codified in the Bill. Nevertheless, it must be emphasised that the Huduma Bill is not law, and is only a draft consultation document.

In India, the Aadhaar Act 2016 specifies its purpose as the assigning of unique identity numbers to individuals, to ensure "transparent and targeted delivery of subsidies, benefits and services." Section 7 of the Act specifically envisages the provision of welfare, stipulating that proof of Aadhaar number/undergoing Aadhaar authentication, may be made necessary for the purpose of establishing the identity of an individual as a pre-condition "for the receipt of a subsidy, benefit or service." The Supreme Court, while upholding the constitutionality of the Act (and reading down or striking down certain sections), held that *"benefits" and "services" as mentioned in Section 7 should be those which have the colour of some kind of subsidies, etc. namely, welfare schemes of the Government whereby Government is doling out such benefits which are targeted at a particular deprived class."* [7]

4 Sections 8(1)(k), (l), (n),(o), Huduma Bill, 2019.

5 Section 17, Huduma Bill, 2019.

6 Section 9(5), Huduma Bill, 2019

7 *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India,* 1 SCC 1, (2019), para 379.1, 511.13.1 ["Aadhaar Judgment"].

In Estonia, the Population Register Act, which governs the issuance of the unique Personal Identification Code, states as its purpose the "collection of reliable information and grant of access to personal data."[8] The Identity Documents Act regulates the issuance of identity documents, which are mandatory for Estonian residents to prove their identity for most government services, including for the "provision of public services."[9] These legislations govern the digital identity framework in Estonia, and therefore have codified the need for provision of welfare or public services in the law. Further, they also lay down the requirement to verify the identity of an ID applicant and ensure its uniqueness — although not in sufficient detail — in the parent legislations itself. *Thus, this use is codified in valid law.*

1.2 LEGITIMATE AIM

Does the law have a legitimate aim?

In Kenya, the object of the Huduma Bill, as per Section 3(d), is to *"facilitate transparent and efficient delivery of public services"* and to that extent, the law has a legitimate aim. This is further supplemented by the Memorandum of Reasons and Objects,[10] which states that the failure to have linkage between foundational and functional systems has led to wastage of resources and diminution of trust in the identity ecosystem.

Similarly, in India, the digital (biometric) ID, Aadhaar, is meant to provide for a transparent and targeted delivery of subsidies, benefits, and services; to ensure that the identity of the person to whom a digital ID is being assigned is not fraudulent; and their identity is unique. This is in furtherance of a legitimate aim, and forms the primary purpose of the ID project. The Supreme Court in the *Aadhaar judgment* held that the Aadhaar Act had a legitimate aim, relying primarily on Section 7 of the Act, while noting that it was *"aimed at offering subsidies, benefits or services to the marginalised sections of the society for whom such welfare schemes have been formulated from time to time" and "the objective of the Act is to plug the leakages and ensure that fruits of welfare schemes reach the targeted population, for whom such schemes are actually meant."*[11]

8 Section 4, Population Register Act, 2019.

9 Section 1, Identity Documents Act, 2000.

10 Memorandum of Reasons and Objects, Huduma Bill, 2019.

11 *Aadhaar Judgment, supra,* paras 314, 373.

The use of digital identity to provide public services, as under the Identity Documents Act in Estonia is a legitimate aim.

The use of digital ID for provision of welfare falls under a legitimate aim.

1.3 DEFINING ACTORS

Does the law clearly define all the actors that can use/ manage or are connected to the ID database in any way, for this use case?

In Kenya, Section 8 of the Huduma Bill lists the mandatory uses of the Huduma Namba which include inter alia transacting in financial markets, opening a bank account, accessing universal health care and social protection services, and benefits from a government housing scheme etc. Thus, it envisages a broad range of actors that *must* use the database. The Act also does not limit or penalise the use of Huduma Namba in any manner. While currently the Bill seems to envision the interoperability of different government databases, it does not in any manner limit/proscribe its use by private actors. For instance, although social protection services will usually be accessed through the State, there is no prohibition in the Bill, if the task of onboarding residents is given to private actors. Consequently, the law does not seem to clearly define the actors that can use or manage or are connected to the NIIMS database.

In India, the provision of welfare is linked to the Aadhaar Act, through Section 7, which restricts it to Central and State governments only. However, the Supreme Court further clarified that not all functions of the Central or State government would be encompassed within the use case for welfare, for the purpose of Aadhaar and instead held that[12]:

a. Benefit which is earned by an individual (e.g. pension by a government employee) cannot be covered under Section 7 of the Aadhaar Act, since that it not in the nature of a welfare benefit; but is rather the right of an individual to receive such benefit.

12 *Aadhaar Judgment, supra,* paras 377-379, 379.1, 379.2, 379.3

b. Only benefits and services which have the colour of some kind of subsidies, etc. namely, welfare schemes of the Government — whereby Government is doling out such benefits which are targeted at a particular deprived class — *and* where the expenditure (for such benefits and services) is drawn from the Consolidated Fund of India, would be covered under Section 7 of the Aadhaar Act.

c. Hence, the Government was not permitted to use the Central Identities Data Repository ("CIDR") or link the Aadhaar number to the provision of scholarships under the UGC or the taking of school leaving or college entrance exams such as CBSE, NEET, JEE, etc.

Apart from this, private actors usually do not service/implement welfare schemes.

In Estonia, the Identity Documents Act seems to permit both public and private actors to provide services to an e-resident with a digital identity card, or to restrict services to ensure its operation or "safe use."[13] Further, in the case of "substantial public interest", the Police and Border Guard Board ("PBGB") may transfer an e-resident's digital identity card to a public agency.[14] The Estonian Notification Form for Electronic Identity Scheme under Article 9(5) of Regulation (EU) No. 910/14 stipulates that the PBGB manages the registration process of the unique personal identification data while the authentication procedure is assured/granted by the PBGB through a subcontracted qualified trust service provider (certification authority). Thus, there is some uncertainty about the exact actors who are connected to the ID database. Similarly, under the Unemployment Insurance Act, the procedure for maintaining the unemployment insurance database (which contains personal data of insured persons) and the processing, use, and issue of data therein is provided for in Regulations, with the only stipulation that the database shall be maintained pursuant to the Personal Data Protection Act and the Public Data Act.[15]

To meet this test, the governing law must specify and restrict the actors who use or control the use of ID for the provision of welfare.

13 Section 20[10], Identity Documents Act, 2000.

14 Section 22(11), Identity Documents Act, 2000.

15 Section 22(11), Identity Documents Act, 2000.

1.4 REGULATING PRIVATE ACTORS

Is this use of the ID system by private actors adequately regulated?

The Huduma Bill in Kenya does not regulate or specifically deal with the use of the ID system by private actors, and thus the extent to which private actors can access the system is unclear. However, the Memorandum of Reasons and Objects notes as one of its objectives "enhanced public *and private sector* service delivery." Further, the use by private actors is not prohibited or disincentivized in any manner in the Bill, and is in fact, contemplated by Section 8. Thus, the use of the ID system by private actors is not adequately regulated under the Bill.

In India, the use of the ID system for the provision of welfare is restricted in the law to the Central and State government. Thus, it does not envisage its use by private actors, although private entities may perform authentication, subject to the conditions prescribed under the amended Section 4(4) of the Aadhaar Act.

The Identity Documents Act in Estonia envisages the provision of services to e-residents by private actors.[16] For instance, the provision of health services through e-estonia healthcare[17] takes place through an online e-Health record, identified by the electronic ID card, which can be tracked by patients, doctors, hospitals, and government. Given that 99% of health data has been digitised in Estonia and 99% of all prescriptions are digital, private actors need to be more strongly regulated. Even the provision of social welfare and social rehabilitation service under the Social Welfare Act, 2015 envisages participation by private actors, who are required to ensure that the processing of sensitive personal data takes place pursuant to the procedure established by the Personal Data Protection Act.[18]

In all these cases, the use of the system by private actors for welfare delivery is insufficiently regulated.

16 Section 20[10](a), Identity Documents Act, 2000.

17 "Healthcare", e-estonia, last accessed May 13, 2020, *https://e-estonia.com/solutions/healthcare/e-health-record.*

18 Section 55(4), 66(6), Social Welfare Act, 2015.

1.5 DATA SPECIFICATION

Does the law clearly define the nature of data that will be collected?

The use of the ID for welfare services must be accompanied by clear specification of the personal data that will be collected and processed.

The Huduma Bill in Kenya prescribes the collection of biometric data, which has been defined to include fingerprint, hand geometry, earlobe geometry, retina and iris patterns, toe impression, voice waves, blood typing, photograph, or such other biological attributes of an individual obtained by way of biometrics.[19] The biometric data of an individual is part of their foundational data, which will be used to attest their identity. Further, the Huduma Namba will be authenticated in the NIIMS database through fingerprints or any other specified biometric data, and can then be used in the absence of the Huduma card.[20]

Vide the Statute Law Miscellaneous (Amendment) Act, 2018, the government amended Sections 3, 5, and 9 of the Registration of Persons Act to provide for the collection of DNA and GPS coordinates for the purpose of identification as one of the mandatory requirements for entry into the register of persons in Kenya. However, in January 2020, the Kenyan High Court found that this collection was intrusive and unnecessary; and to the extent that it was not authorised and specifically anchored in empowering legislation, it was unconstitutional and a violation of Article 31 of the Kenyan Constitution.

In India, the Aadhaar Act provides for the collection of biometric information and demographic information. Biometric information has been defined as *meaning* "photograph, finger print, Iris scan, *or such other biological attributes of an individual as may be specified by regulations."* [21] Demographic information has been defined as *including* "information relating to the name, date of birth, address and other relevant information of an individual, *as may be specified by regulations* for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical

19 Section 2, Huduma Bill 2019.

20 Section 9(6), Huduma Bill, 2019.

21 Section 2(g), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 ["Aadhaar Act"]. Additionally, Section 2(j) further defines Core biometric information" as meaning fingerprint, iris scan, or such other biological attribute of an individual as may be specified by regulations.

history."[22] The Aadhaar (Enrolment and Update) Regulations[23] provide some more specification about the nature of biographic and demographic information that will be collected at the time of enrolment. Thus, although both the terms biometric and demographic information are defined, they leave room for the State to prescribe — by way of executive action, through the notification of regulations — further types of information that can be collected.[24]

In Estonia, the list of data to be entered in a document under the Identity Documents Act is to "be established by a regulation of the minister responsible for the area," and may include date and place of birth, photo, fingerprint images, hair colour, iris images, personal identification code.[25] The Minister of Interior has consequently issued Regulation 77 to deal with the collection of the relevant identity data required for identity proofing and verification. Although the translated version of the Regulation 77 is not available online, it has been reported that it prescribes the collection of personal data, citizenship, contact information, place of issuance, reason for applying and date. No collection of biometric information seems to have been prescribed under the Regulation.[26] Apart from this, Section 9(2) of the Act envisages the collection of biometric data, for procedures that are specified under the Act, which may be processed only in the cases and under the conditions provided by law.

22 Section 2(k), Aadhaar Act, 2016.

23 Regulations 3-5, Aadhaar (Enrolment and Update) Regulations, 2016.

24 In the Aadhaar judgment, it was observed that applying the principle of ejusdem generis, the phrase "such biological attributes" has to be construed by applying the principles of ejusdem generis, meaning that the biological attributes, which can be added by the Regulations, have to be akin to one those mentioned in Section 2(g) i.e. photographs, fingerprints and iris scan. This saved the section from being struck down as unconstitutional. However, in his dissent, Justice Chandrachud noted that although the Act specifically provided for what information could be collected, it did not specifically prohibit the collection of further biometric information. He stated: *"The definitions of these sections provide the Government with unbridled powers to add to the list of biometric details that UIDAI can require a citizen to part with during enrolment which might even amount to an invasive collection of biological attributes including blood and urine samples of individuals."*

25 Section 9, Identity Documents Act, 2000.

26 Republic of Estonia, Police and Border Guard Board, *Estonian eID scheme: ID card: Technical specifications and procedures for assurance level high for electronic identification* (2018), at 7, 33.

1.6 USER NOTIFICATION

Does the ID system provide adequate user notification mechanisms for this use case?

Users should be notified when their data is used or accessed, and when a data breach has occurred.

In Kenya, the ID system does not notify users while using their data for the purpose of welfare delivery. Residents are only informed in case of data breach when "there is a real risk of harm to the enrolled person whose personal data has been subjected to the unauthorised access."[27]

In India, although the law itself does not provide for a user notification system for the purpose of welfare delivery, the Aadhaar (Authentication) Regulations[28] stipulates that users "may" be notified of any biometric and/or OTP based authentication, through their registered email and/or mobile number,[29] at the time of authentication. However, it is not clear if this notification process is mandatory, and whether it includes authentication done at the instance of welfare delivery. Further, the Act does not provide for any user breach notification, in case of unauthorised access by third parties.

There does not seem to be any provision for adequate user notification mechanism in the Identity Documents Act in Estonia for the provision of public services. However, Section 12 of the Personal Data Protection Act requires notifying data subjects in case their data is being processed, and Section 15 prescribes user notification if the source of the personal data is any other than the data subjects themselves.

27 Section 43(1), Huduma Bill, 2019.

28 Regulation 10 r/w Regulation 5, Aadhaar (Authentication) Regulations, 2016.

29 As per Regulation 4(2) of the Aadhaar (Enrolment and Update) Regulations, mobile number and email address are optionally collected, at the instance of the person undergoing the enrolment.

1.7 USER RIGHTS

Do individuals have rights to access, confirmation, correction and opt out?

In Kenya, Section 36 read with Section 40 of the Huduma Bill, provides individuals with a right to access,[30] confirmation, and correction, while Sections 16 and 24 impose onerous duties to continually update one's particulars in case of any change. However, no further details are provided regarding the procedures for exercising these rights, except to state that the Permanent Secretary shall "facilitate technologically efficient means to ensure proactive access to personal data" to enrolled individual provided in NIIMS database.[31] The First Schedule too, requires recording *"date of every application by the individual for a modification of any individual's entry; date of every application by the individual confirming the contents of the entry or entries made in the database."* Nevertheless, the procedure for making such applications has not been provided under the Bill. There is also no provision to deal with cases of duplicate or contradictory records. Additionally, since the use of the Huduma Namba is mandatory in order to access specified public services, there is no provision for opt out.[32] It has been reported[33] that the Kenyan government has not made public any information regarding its assessment of the accuracy of the data contained in the databases that will be linked to NIIMS.

In India, the Aadhaar Act provides for a right to access information,[34] including identity information, except core biometric information.[35] In the context of welfare delivery, individuals also have the right to access their authentication record.[36] Correction, or "updation" of information, is also provided for under the Act.[37] However, there is no provision of opt out of the authentication process for the receipt of welfare (i.e. benefits, subsidies, or services), since under Section 7 r/w newly inserted Section 4(7), the Central or State Government can make

30 See also Sections 11(6)(d) and 37, Huduma Bill, 2019.

31 Section 37(2), Huduma Bill, 2019.

32 Section 8, Huduma Bill 2019.

33 Open Society Justice Initiative, *Kenya's National Integrated Identity Management System, https://www.justiceinitiative.org/uploads/8f3b665c-93b9-4118-ad68-25ef390170c3/briefing-kenya-nims-20190923.pdf.*

34 Section 3(2)(c), Aadhaar Act, 2016 r/w Regulation 9(c), Aadhaar (Enrolment and Update) Regulations, 2016.

35 Proviso to Section 28(5), Aadhaar Act, 2016.

36 Section 32(2), Aadhaar Act, 2016, read with Regulation 18(2) and 28(1), Aadhaar (Authentication) Regulations, 2016.

37 Section 31(1), Aadhaar Act, 2016, r/w Chapter IV,Aadhaar (Enrolment and Update) Regulations, 2016.

the proof of Aadhaar number mandatory. The only exception is in the case of children, who, pursuant to the Supreme Court's judgment[38] and the amendment to the Aadhaar Act,[39] cannot be denied any subsidy, benefit, or service under Section 7 for failure to furnish an Aadhaar.

Chapter 8 of the Population Register Act in Estonia deals with the rights and procedure concerning access, with Section 44 granting an adult the right to access data in the Population Register pertaining to them, their minor children or wards, and their deceased spouse. Apart from this, Section 45(2) also permits a person to obtain information from a processor about the purpose and legal bases of the processing of data and state and local government agencies and other natural and legal persons who have the right to access data in the population register. Rectification or correction of data is contemplated under Section 31(2) read with Sections 32 and 33 of the Act. There does not seem to be any opt out of the process of use of digital ID for provision of welfare, since the provision of public service can be refused under the Identity Documents Act to a person who refuses to use the certificate enabling digital identification or digital signing.[40] Apart from this, Chapter 3 of the Personal Data Protection Act grants such rights of access, rectification, and deletion.

In all these cases, ID holders using their IDs for accessing welfare services have limited user rights.

1.8 REDRESSAL MECHANISM

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of their rights arising from this use of digital ID?

The institution of redressal mechanisms, that can be accessed at every instance of ID holders' rights being violated, is always an important safeguard, but takes on special importance at the stage of welfare delivery, since access to rights, public services, and benefits is dependent on the successful authentication of the digital ID.

38 *Aadhaar Judgment, supra,* paras 391-391.6.

39 Newly inserted Section 3A(3) of the amended Aadhaar Act, 2016.

40 Section 5(1) read with 18(3), Identity Documents Act, 2000.

In Kenya, the Huduma Bill does not envisage any civil or criminal redressal mechanism in case of exclusion or any other violation of rights caused by the use of the digital ID for the provision of welfare. Section 52, which penalises the unauthorised disclosure, submission, and transfer of data by a NIIMS registration officer from the NIIMS database to another person may be invoked by an aggrieved resident in case this data relates to foundation or functional data created during authentication for receiving benefits. The dispute resolution mechanism set up under Section 59 is only for persons aggrieved by "any decision" under the Act, and does not seem to extend to a violation of their rights arising from the use of the Huduma card for welfare delivery.

In India, the Aadhaar Act stipulates that (a) a child shall not be denied any subsidy, benefit or service under Section 7 in case of failure to establish her identity using Aadhaar,[41] and (b) that in case of an authentication failure (for a variety of reasons), the requesting entity shall, provide such alternate and viable means of identification of the individual, as may be specified by regulations.[42] As long as Aadhaar authentication is not made mandatory by a law made by Parliament, an Aadhaar number holder cannot be denied any service by a requesting entity for refusing to, or being unable to, undergo authentication.[43] However, the Act does not provide any specific remedies, including appeal or compensation, for persons who have been wrongfully suffered exclusion on account of Aadhaar related authentication failures. Under Section 33A, an entity in the Aadhaar ecosystem will be liable for a civil penalty of up to INR 1,00,00,000 for any contravention with the provisions of the Act, Rules, Regulations, or UIDAI direction. Even then, any adjudication under Section 33A will take place by an inquiry, which can be initiated only at the behest of the UIDAI (and not the aggrieved Aadhaar number holder).[44]

The issuance of a document is a pre-condition for availing public services in Estonia. An identity number is not granted if the applicant cannot be verified.[45] The framework does not establish any review mechanism that rejected applicants can turn to if grant of identity number is refused. In case of revocation of document, the authority which has revoked the document shall inform the holder of the document of the revocation of the document without undue delay.[46] There does not seem to be any provision for the holder of the document to contest

41 Newly inserted Section 3A(3) of the amended Aadhaar Act, 2016.

42 Proviso to the amended Section 8(2)(b), Aadhaar Act, 2016.

43 Section 4(6) r/w 4(7), Aadhaar Act, 2016.

44 Section 33B, Aadhaar Act, 2016.

45 Sections 11, 12, Identity Documents Act, 2000.

46 Section 13 r/w 20, Identity Documents Act, 2000.

the revocation. Further, under Section 15 of the Identity Documents Act, the Minister responsible for the area shall issue Regulations for the for the procedure for identification and verification of the identity of an applicant for an identity card, and digital identity card. The PBGB shall issue and revoke a digital ID card. No provisions of redress have been prescribed against such actions, or in case individuals are denied access to a service on account of failure of enrolment or identification, under the Identity Documents Act.

1.9 ACCOUNTABILITY

Is there an independent/adequate regulatory mechanism to ensure accountability of the administrator of the digital ID?

In Kenya, the law does not identify any regulatory mechanism to govern the administrator (the Principal Secretary/Cabinet Secretary) of the digital ID while using it in relation to welfare delivery. In fact, the Principal Secretary has been granted a lot of power — including the power to appoint a data protection officer,[47] cancel enrolment,[48] and facilitate technologically efficient means to promote access[49] — without any accountability. There is no independent authority running the NIIMS database, nor has any level of parliamentary, judicial, or executive oversight been provided. Neither the administrator nor the government agencies or private entities can be held accountable for data breaches.

Further, Section 10 of the Bill requires the Cabinet Secretary to ensure that the NIIMS structure and design of the NIIMS is output oriented, technology neutral, flexible, and has no technology lock-ins by any vendor. However, no accountability or grievance mechanism has been prescribed to ensure compliance with this provision. Instead, the onus seems to have been shifted completely on the residents to successful enrol — any failure to enrol (owing to social, cultural, or political barriers) that results in an individual taking the benefit of any health, education, or other service will result in them being criminally prosecuted.[50]

47 Section 45, Huduma Bill, 2019.

48 Section 25, Huduma Bill, 2019.

49 Section 37, Huduma Bill, 2019.

50 Section 48, Huduma Bill, 2019.

In India, although the UIDAI — the executive body designated as an Authority under the Act — can be held financially accountable,[51] it is not regulated or held accountable in any way for the process of disbursing welfare through Aadhaar or for any exclusion that has been caused by an error or failure in Aadhaar authentication. No performance audit of the UIDAI is carried out at the end of the year.[52] Consequently, there is limited oversight or transparency in the welfare delivery process under Section 7 of the Aadhaar Act. The situation is exacerbated by the fact that UIDAI serves both as an administrator of the digital ID (by overseeing the collection and storage of the identity information of all residents and the authentication and offline verification process etc.) and a regulator (by issuing binding directions, notifying regulations etc.), thus being liable to be faced with a situation involving a conflict of interest.

In Estonia, there is no other authority or body identified by the digital ID framework besides the administrator. The Public Information Act, which has been governing public sector databases since an amendment in 2008, gives supervisory control for determining compliance with the Act to the Data Protection Inspectorate and the Estonian Information System Authority; however, this is primarily concerned with the maintenance of the database of information, and does not extend to the process of verification in issue of ID. Further, it applies only to the public sector, notwithstanding that the private sector also maintains databases connected to the same infrastructure and leveraging the Digital ID. Thus, there is no accountability mechanism in place to govern the process of verification for provision of services. Section 15 of the Identity Documents Act classifies the PBGB as the controller of the identity documents Database, while Section 20 states that the PBGB, the Estonian Internal Security Service and the Estonian Tax and Customs Board are competent to exercise state supervision over the use of the e-resident's digital identity card. However, no further accountability mechanism seems to be prescribed.

There is an urgent need for adequate redressal mechanisms, either through the ID law or a data protection law, especially for uses as important as welfare delivery.

51 Section 26(1), Aadhaar Act, 2016.

52 See also Vrinda Bhandari and Renuka Sane, 'A Critique of the Aadhaar Legal Framework' 31(1) NLSI Rev 72 (2019).

1.10 DEFINING PURPOSES

Does the governing law explicitly specify the proposed purposes of the digital ID?

In Kenya, Section 8 of the Huduma Bill read with the Memorandum of Reasons and Objects explicitly specifies the various proposed purposes for the digital ID, whereas Section 17 explains the linkage between the foundational and functional data.

In India, the proposed purpose for the digital ID (Aadhaar) has been specified in the Act, namely, for establishing the identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure has been incurred from the Consolidated Fund of India or the State.[53] The powers and functions of the UIDAI include *"specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and* ***other purposes*** *for which Aadhaar numbers may be used."*[54] The phrase "other purpose" has been interpreted by the Supreme Court to require a relation to subsidies, benefits and services mentioned in Section 7 and be confined only to that purpose when it is chargeable to the Consolidated Fund of India.[55]

In Estonia, Section 5 of the Identity Documents Act makes it mandatory for an Estonian citizen above the age of 15 years to hold an identity card. Section 20[5] stipulates that *"the objective of the issue of an e-resident's digital identity card is to promote the development of the Estonian economy, science, education or culture by providing access to e-services with the Estonian digital document."* Thus, the purpose of welfare delivery and provision of services is clear from the law.

In all these cases, the proposed purpose for the Digital ID, for the delivery of welfare services, is explicitly specified in the governing law.

53 Section 7, Aadhaar Act, 2016.

54 Section 23(2)(h), Aadhaar Act, 2016.

55 *Aadhaar Judgment, supra,* para 468.

1.11 MISSION CREEP

In case there are newer purposes identified, are there regulatory procedures in place to determine their legitimacy?

In Kenya, Section 8 of the Huduma Bill specifies the cases where there is a mandatory obligation to present a Huduma Namba. Any new purpose that is identified can be integrated with the Huduma Numba by notifying it under Section 8(q)'s ambit of "any other specified public service." The only regulatory procedure put in place to determine the legitimacy of a newer purpose is that personal data collected under the Act should not be used for an "unlawful purpose."[56] There is no provision to deal with a change or extension of purpose from the one originally identified.

In India, there are no provisions in place to have a process for determining the appropriateness or legitimacy of new uses and purposes. In the past, the purpose for the use of Aadhaar was made clear through various notifications issued by the Central or State Government that mandated Aadhaar authentication for the receipt of a certain specific benefit, subsidy, or service such as social security pension or PDS (Public Distribution System).[57]

There do not seem to be any regulatory procedures in place under the Identity Documents Act in Estonia to deal with new purposes, as long as they are covered under Section 20[10].

By failing to have restrictions against additional uses of the ID, or governance mechanisms for new uses, the ID system is not protected against mission creep.

56 Section 37(1), Huduma Bill, 2019.

57 The Supreme Court in the *Aadhaar judgment* narrowly interpreted the definition of "benefit, subsidy or service" under Section 7 of the Act and thus struck down the notifications making Aadhaar mandatory for school/entrance exams under CBSE/JEE. See *Aadhaar judgment, supra,* para 379.

RIGHTS BASED TESTS

2.1 DATA MINIMISATION

Are principles of data minimisation followed in the collection, use, and retention of personal data for this use case?

The principles of data minimisation are respected where only such data as is relevant and necessary for the purpose of establishing identity or detecting fraud, has been collected and processed.

Even the period and purpose of storage of the information collected should be analysed through the lens of data minimisation.

In Kenya, at the time of enrolment into NIIMS, every resident has to provide foundational data (including photographs, fingerprints, and "any other biometric data"), personal reference numbers (including tax payer, driving license details, National Hospital Insurance Fund number, National Social Security Fund number, National Education Management Information System number), and registration history.[58] Principles of collection limitation, thus, do not seem to complied with, especially since the provisions of the Huduma Bill are not clear on what can be collected as part of "any other biometric data". Even the restrictions on data sharing[59] in the Bill do not prescribe any purpose or use limitation. Additionally, the Bill fails to restrict the access of government agencies delivering a public service (which shall be linked to the NIIMS database),[60] to the vast trove of personal data present in the NIIMS database. Thus, although the Memorandum of Reasons and Objects states that Part V of the Huduma Bill sets out data protection safeguards accorded to NIIMS, and adopts international best principles under the GDPR, the principles of data minimisation do not seem to have been explicitly or implicitly followed in the case of collection, retention, or use of personal data for the provision of welfare.

58 Section 6 r/w 11 r/w First Schedule, Huduma Bill, 2019.

59 Section 38, Huduma Bill, 2019

60 Section 17(2), Huduma Bill, 2019.

In India, the Supreme Court held that principles of data minimisation have been "largely followed" under the Aadhaar Act,[61] relying on three factors — (i) the collection of photographs and demographic information, did not raise any reasonable expectation of privacy, especially given the prohibition of collection of certain specified types of demographic information under Section 2(k); (ii) minimal biometric data in the form of iris and fingerprints is collected during enrolment, and no purpose, location or details of the authentication transactions are collected; and (iii) Section 32(3) of the Act and the proviso to Regulation 26 of the Authentication Regulations specifically prohibited the UIDAI from collecting, storing or maintaining, either directly or indirectly any information about the purpose of authentication.[62] However, keeping in mind data protection principles, the Court, *inter alia* ruled that —

i. Authentication records are not to be kept beyond a period of six months, as stipulated in Regulation 27(1) of the Authentication Regulations; and that the provision, which permits records to be archived for a period of five years was held to be bad in law.[63]

ii. The storage and maintenance of metadata relating to the authentication transaction by the UIDAI under Regulation 26(c) of the Authentication Regulations was impermissible in its present form and needed a suitable amendment.[64]

In Estonia, the population register collects detailed information about an individual, including their personal identification code, marital status, information about their family, and custody and guardianship details (if any), educational, ethnicity, and mother tongue.[65] Apart from this, information about various documents is also entered into the population register, such as personal identification document; marital status certificate; individual's notice about their data. All this information is stored/ preserved "for an unspecified term." [66] Even after the information loses relevance (e.g. if a person dies), it is not deleted, but is instead transferred to the archives of the register. In case of e-residents, information regarding their criminal histories, social media accounts, etc is also taken. Further, fingerprints of the e-resident applicant are taken, even though

61 *Aadhaar judgment, supra,* para 229.

62 *Aadhaar Judgment, supra,* paras 227-228, 510.2.1.

63 *Aadhaar Judgment, supra,* para 510.4.1, 513.3

64 *Aadhaar Judgment, supra,* para 510.4.2.

65 Sections 21, 22, 105, Population Register Act, 2019.

66 "Population Register," Republic of Estonia Ministry of the Interior, last accessed May 13, 2020, *https://www.siseministeerium.ee/en/population-register*.

there is no recorded use of it for verification or authentication. Thus, the excessive collection of data, particularly with no stated purpose, does not comply with principles of data minimisation.

Additionally, in accordance with the Statutes for the Maintenance of the Identity Documents Database, the following information is recorded in the identity documents database on an application for digital identity (apart from that submitted with the application —) data of commencement of identification, reasons for application, manner of identification and reason for the identification procedure, name & number of other identity documents issued to the person, etc. The storing of all above mentioned data at the stage of identification is not in consonance with the principles of data minimisation. Thus, principles of data minimisation are not followed.

2.2 ACCESS TO DATA

Does the law specify access that various private and public actors have to personal data in this use case?

In Kenya, the Huduma Bill is silent on provisions regarding access (by public or private actors) to the NIIMS database for the purpose of welfare delivery. No specific prohibitions or restrictions regarding access by different actors have been spelt out in the Act.

In India, the Aadhaar Act does not specifically deal with the access that private and public actors have to personal data/identity information in the case of welfare delivery. However, it is clear that core biometric information (i.e. finger print and iris scan) of an individual collected under the Act, shall not be shared with anyone for any reason whatsoever.[67] Section 29(3), as amended, provides that no identity information, available with a requesting entity or offline verification seeking entity, shall be used for any purpose, other than the purposes informed in writing to the individual at the time of submitting their information. The Regulations suggest that the sharing of Aadhaar number, which is contained in a public (welfare) database, is prohibited.[68] Further, any identity information that is available with a requesting entity (e.g. during authentication) shall not be used by it for any purpose other than that specified to the Aadhaar number holder at the

67 Section 29(4), Aadhaar Act, 2016, r/w Regulation 3(1), Aadhaar (Sharing of Information Regulations), 2016.

68 Regulation 6, Aadhaar (Sharing of Information Regulations), 2016.

time of submitting their information; and this information shall not be disclosed further without the prior consent of the Aadhaar number holder.[69]

In Estonia, Section 44 of the Population Register Act grants state and local government agencies access to data entered into the population register "for the performance of public duties," while also permitting such access to natural and legal persons "with a legitimate interest." Legitimate interest has been defined as "the protection of the life, health, rights and freedoms of the applicant or another person," "performance of a contract entered into with the applicant or for ensuring performance of the contract."[70] However, the law also provides for restriction of access under certain conditions. In general, thus, access has been provided to both public and private actors, for the provision of welfare, as long as they meet the aforementioned criteria. This is also the case with the provision of social welfare wherein the providers of social services such as the providers of safe house service, substitute home service etc. have access to the data[71] contained in the centralised database — the Social Services and Benefits Registry.[72]

To meet this test, the governing law must specify the nature of actors that have access to the personal data generated in the system, and/or have a manner to regulate such access.

2.3 EXCLUSIONS

Is the use of digital ID to access services exclusionary in this use case?

The NIIMS database in Kenya is intended to serve as a single source of both foundational and functional data for enrolled residents, and to enable the use of fingerprints and other biometric data to identify an enrolled person.[73] Section

69 Regulation 4(2), Aadhaar (Sharing of Information Regulations), 2016.

70 Section 46 r/w 51, Population Register Act, 2019.

71 This data includes the name, personal identification code, date of birth, date of death and sex of the person; their status in the population register and residence; and the data entered by the administrative authority concerning the provision of the social service the person has been referred to receive. See Section 145, Social Welfare Act, 2015.

72 Section 142, Social Welfare Act, 2015.

73 Section 6(3), Huduma Bill, 2019.

9(6) envisages the authentication of the Huduma Namba by the NIIMS database through fingerprints or "any other specified biometric data". However, the Bill does not provide for any alternative mechanisms in the event the ID is rejected (if de-duplication or authentication fails or if the fingerprint changes with age and manual labour) or if enrolment is unsuccessful (owing to social or cultural barriers, faced for instance, by Nubians). This, combined with the fact that the ID is compulsory to access a host of government services, the centralisation of all registration system, and that all other existing forms of ID not issued under the NIIMS Act are replaced by the Huduma Namba,[74] is exclusionary. The impact of exclusion is likely to be exacerbated by the centralised nature of the digital ID; and the fact that residents do not have the option of registering with another substitute digital ID like is the case in Canada or the UK, etc.

In India, while the possession of a digital ID (Aadhaar) is not mandatory, it is required or mandatory for the present use case of accessing subsidies, benefits, and services under Section 7. Aadhaar based biometric authentication to access welfare benefits can be exclusionary due the following factors: (i) probabilistic nature of biometric authentication (which gets exacerbated with age, class, manual labour, and disability), (ii) structural capacity constraints (such as poor internet and mobile access), (iii) machine errors (e.g. in the fingerprint recognition software), (iv) manual seeding errors (which requires the name, demographic information, and Aadhaar number to be correctly and identically recorded across databases).[75] In line with the judgment of the Supreme Court,[76] the Aadhaar Amendment Act provides that no person shall be denied any service to him for refusing to, or being unable to, undergo authentication.[77] However, as a matter of practice, the issue of exclusion persists. In a recent study published in February 2020, researchers found, in a randomised control experiment involving 15 million beneficiaries in Jharkhand, that by itself, requiring biometric authentication to transact did not reduce leakage, slightly increased transaction costs for the average beneficiary, and reduced benefits received by the subset of beneficiaries who had not previously registered an ID by 10%. They concluded that Aadhaar-based biometric authentication had led to "non trivial" costs

74 Section 8 r/w 6(4) r/w 9(5), Huduma Bill, 2019.

75 Jean Dreze *et al,* "Aadhaar and Food Security in Jharkhand: Pain Without Gain?", 52(50) *EPW* (2017); Anmol Somanchi *et al,* "Well Done ABBA?", 52(7) *EPW* (2017).

76 Incidentally, the Supreme Court made it clear that the Aadhaar Act cannot be invalidated only on the ground of possibility of exclusion by some of the seekers of the welfare scheme. See *Aadhaar judgment, supra,* para 373.

77 Section 4(6), Aadhaar Act, 2016, as amended.

in terms of exclusion.[78] Similarly, in a third party report, "State of Aadhaar — 2019,"[79] based on pulse survey of 1.47 lakh respondents and an in-depth survey of 19,209 respondents, it was found that 2.5% of all respondents experienced exclusion from a key welfare service — they could not access it at all. One-third of them (0.8%) previously had accessed the service. Non-Aadhaar related reasons contributed to exclusion from services for several times as many people (22% experienced exclusion for non-Aadhaar related reasons; 3.5% experienced exclusion for non-Aadhaar related reasons from a service they had earlier received). The Report also found that marginalised groups, such as homeless and third-gender people, are disproportionately represented among those who face Aadhaar-related exclusion from services, such that these two groups were nearly one-third as likely to have access to PDS rations without Aadhaar than with Aadhaar.[80] Authentication errors, manual errors and capacity challenges pose significant difficulties, and they all could lead to high human costs of exclusions.

In order to reduce exclusionary impact, it is imperative that access to welfare services is not made contingent on a mandatory authentication through the digital ID.

78 Karthik Murlidharan et al, "Identity Verification standards in welfare programs: experimental evidence from India," *NBER,* (2020), *https://faculty.virginia.edu/sandip/MNS%20JH%20ABBA.pdf*

79 Dalberg, "State of Aadhaar: A People's Perspective", 18-19, (2019), *https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf* ["State of Aadhaar"].

80 *State of Aadhaar, supra,* at 15, 18.

RISK BASED TESTS

3.1 RISK ASSESSMENT

Is this use case regulated taking into account its potential risks?

The **Kenyan** model of interoperability of public and private databases with the NIIMS database, and its exclusive reliance on the data stored therein for verification, does not seem to take into account the risks of breach of data, poor security, inaccurate data, failure of system, etc. In fact, by specifying that NIIMS shall operate as a single source of personal identification for citizens and persons resident in Kenya,[81] the Bill only increases the risk of linking all data, and access to all services, to a single document. The use case has not taken into account the risk of failure to enrol, due to a variety of social, cultural, political factors, and the consequence of being deprived of access to government services. Further, the use of biometrics and fingerprints as identifiers means that if such data is stolen or lost, it cannot simply be replaced, and will result in increasing the burden on the residents. Section 17 of the Bill relates to the supply of functional data into NIIMS and requires every government agency delivering a public service to authenticate personal data in their possession with NIIMS. However, it does prescribe the method of authentication (e.g. whether it is biometric or mobile based OTP authentication) and does not deal with a situation where the authentication fails, resulting in impediments to the delivery of service. There is no offline or OTP based enrolment and authentication process. *The governing law is also completely lacking in terms of identifying, handling, and mitigating such risks.*

In India, there does not seem to be an adequate consideration of risk based factors in the Aadhaar Act, particularly on account of exclusion caused by failure of Aadhaar-based biometric authentication. Mitigation strategies (described below) were employed many years after reports of authentication failures emerged. Although the success of Aadhaar and biometric authentication depends on every person being correctly seeded in the CIDR, it is not clear how authentication can correctly verify the identity of an individual using “offline” measures or through OTP-based authentication (that simply depends on a mobile phone number and/or email address).[82] Apart from this, the administrator of the system, the UIDAI, is not accountable for the denial of welfare caused by the

81 Section 4(2), Huduma Bill, 2019.

82 Regulation 4(2)(b), Aadhaar (Authentication) Regulations, 2016.

failure of Aadhaar-based biometric authentication, and applicants have limited recourse against the administrator. Thus, there are several glaring risks that seem to have gone unaccounted for in the governance of the system.

The risk assessment that seems to have been done in Estonia is to permit an individual to apply for their identity document to be issued with or without biometric data.[83] Fingerprints of an individual shall not be captured if they lack all fingers or the state of their health renders them unable to undergo fingerprinting.[84] Further, the law prescribes digital identification in a digital identity card or in a mobile ID format,[85] instead of biometric authentication, as a means of identification, and to that extent, takes into account the dangers of biometric authentication. The use factors also takes into account the risks caused by biometric authentication by instead prescribing two factor authentication for using the Estonian ID card eID — a chip ID card and PIN codes. This electronic identification helps prevent against duplication, without incurring the risks of biometric authentication.[86]

The use of the digital ID for providing welfare services must be accompanied with proper risk assessment, which seems to be lacking in the above cases.

3.2 PRIVACY RISK MITIGATION

Is there a national data protection law in place?

Kenya does not currently have a functioning data protection law in place. The Data Protection Act, 2019[87] was passed in November, and envisages the establishment of the office of the Data Protection Commissioner. However, it is not clear how long it will take for this body to become operational and for the appointment of a commissioner to head it.[88] The Kenyan High Court permitted the government to

83 Section 11^{2}-11^{5}, Identity Documents Act, 2000.

84 Section 11^{6} of the Identity Documents Act, 2000.

85 Section 20, Identity Documents Act, 2000.

86 Republic of Estonia, Police and Border Guard Board, *Estonian eID scheme: ID card: Technical specifications and procedures for assurance level high for electronic identification* (2018), at 11.

87 Data Protection Act, 2019.

88 "Huduma Namba: Kenya Court halts biometric ID over data fears", *BBC News,* January 31, 2020, *https://www.bbc.com/news/world-africa-51324954*

proceed with the implementation of NIIMS on the condition that *"an appropriate and regulatory framework on the implementation of NIIMS, that is compliant with the applicable constitutional requirements... be enacted."*[89]

India does not currently have a national data protection law. However, the Personal Data Protection Bill is likely to be placed before the Indian Parliament in the Budget/Winter Session of 2020-21, having been referred to the Joint Parliamentary Committee. Currently, there exists a set of rules that govern protection of sensitive and personal data, but it applies only to body corporates incorporated in India that collect data, and would not apply to actions of the Government or of Government bodies or agencies.

Estonia has a Personal Data Protection Act, 2007, which has established a Data Protection Inspectorate.

The presence of a robust data protection framework, particularly one with an independent regulator, adequately reduces the risk of the ID system.

3.3 PRIVACY BY DESIGN

Are there privacy by design systems that minimise the harms from data breach etc?

In Kenya, Section 10 of the Huduma Bill 2019, merely requires the Cabinet Secretary to ensure *"the structure and design of the NIIMS is output oriented, technology neutral, flexible, and has no technology lock-ins by any vendor."* Apart from this vaguely worded requirement, there is no further specification of privacy by design systems that have been identified to minimise the harms from data breach.

In India, the UIDAI introduced the Virtual ID (VID), which is a temporary, revocable 16-digit random number mapped with the Aadhaar number. VID was meant to be used in lieu of Aadhaar number whenever authentication or e-KYC services are performed. Authentication may be performed using VID in a manner similar to using Aadhaar number. The UIDAI clarified that it was not possible to derive Aadhaar number from VID.[90] The Aadhaar Amendment Act amended

89 *Nubian Rights Forum and Ors v. Attorney General of Kenya and Ors,* Consolidated Petitions No. 56, 58 & 59 of 2019, Constitutional and Judicial Review Division, High Court of Kenya (2020).

90 Circular No. 1/2018, UIDAI, January 2018, *https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf*.

the definition of Aadhaar number under Section 2(a) of the Act to include "any alternative virtual identity" that had been generated under Section 3(4) of the Act.[91] However, till date, no Regulations have been notified by the UIDAI under Section 3 to elaborate on the procedure for generating an alternative virtual identity. The UIDAI also introduced the concept of a UID Token, which is a 72 character alphanumeric string meant only for system usage.[92] Under this system, the token would remain the same for an Aadhaar number for all authentication requests by a particular entity (AUA/Sub-AUA). However, for a particular Aadhaar number, different AUAs/sub-AUAs would have different UID tokens.

The privacy by design requirement that has been built into the Estonian id card system is the that of two factor authentication using a chip ID card (which requires possession of the chip ID card) and PIN codes (which requires knowledge of the unique private key, which is used for authentication).[93]

Overall, privacy by design and other risk strategies were inadequately considered in the design of the ID system and its governing law.

91 Section 3(4) clarified that the Aadhaar number included "any alternative virtual identity as an alternative to the actual Aadhaar number..." that was to be generated by the UIDAI in the manner specified by Regulations.

92 Circular No. 01/2018, UIDAI, January 2018, *https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf*

93 Republic of Estonia, Police and Border Guard Board, *Estonian eID scheme: ID card: Technical specifications and procedures for assurance level high for electronic identification* (2018), at 11.

3.4 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure/ breach of the ID system?

A mitigation strategy is important to ensure an effective response to failures or breaches in the ID system.

In Kenya, the governing law, the Huduma Bill 2019 does not reflect any mitigation strategy accounting for situations of failure or breach of the system. The only safeguard seems be an option for an individual whose Huduma card has been "otherwise rendered unserviceable" to apply for a replacement,[94] although whether failure to authenticate will be included within this is unclear. The Cabinet Secretary has been tasked with developing mitigation strategies on legal, procedural, and social barriers to enrolment, although the Bill does not expressly deal with this challenge. Further, there is no similar mandate to mitigate the failure or breach of the Huduma Namba while accessing public services or welfare delivery.

In India, to reduce the risk of exclusion caused by the failure of the authentication of the ID system (Aadhaar), the Cabinet Secretariat had released an Office Memorandum[95] detailing an "exception handing" mechanism. The Memorandum created the following mechanism for availing subsidies, benefits or services in cases where Aadhaar authentication fails:

(i) Departments and bank branches may make provisions for iris scanners along with fingerprint scanners wherever feasible;

(ii) in cases of failure due to lack of connectivity, offline authentication systems such as QR code based coupons, mobile based OTP or TOTP may be explored; and

(iii) in all cases where online authentication is not feasible, the benefit or service may be provided on the basis of possession of Aadhaar, after duly recording the transaction in a register, to be reviewed and audited periodically.

A proviso was also added to the Aadhaar Act which made it clear that in case of failure to authenticate due to illness, injury or infirmity owing to old age or otherwise or any technical or other reasons, the request entity shall provide such alternate and viable means of identification of the individual, as may be specified

94 Section 15(1), Huduma Bill, 2019.

95 Office Memorandum, DBT Mission, December 19, 2017, *https://dbtbharat.gov.in/data/om/Office%20Memorandum_Aadhaar.pdf*.

by regulations. However, no corresponding regulations have been notified. The Aadhaar Amendment Act has further provided statutory backing to the idea of "offline verification," 96 which is the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes, as will be specified by regulations. The Act also recognises the right of the Aadhaar number holder to establish their identity through offline verification. An Aadhaar number holder seeking offline verification cannot be subject to authentication.

In Estonia, when a security flaw in around 750,000 national Digital ID cards came to light in 2017, making the ID cards susceptible to identity theft, the government took immediate preventive action and declared that the security certificates of the ID cards would be disabled.[97]

96 Section 2(pa) r/w 4(3) r/w 8A, Aadhaar Act, 2016.

97 "What we learned from the eID card security risk?," e-estonia, last accessed January 22, 2019, *https://e-estonia.com/card-security-risk/*.