

GOVERNING ID

Kenya's Huduma Namba Programme

A project of the Centre for Internet and Society, India supported by Omidyar Network

→ digitalid.design ←

→ cis-india.org ←

RESEARCH & WRITING

Amber Sinha

REVIEW & EDITING

Shruti Trikanad

WITH INPUTS FROM

Diana Gichengo

DESIGN

Pooja Saxena

COVER ILLUSTRATION

Akash Sheshadri



Shared under
Creative Commons Attribution 4.0 International license

INTRODUCTION

This is the fourth 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 looks at the Huduma Namba scheme in Kenya.

The National Integrated Identity Management System (NIIMS) is intended as a foundational identity system to set up and manage a national population register as a single source of information about all citizens and residents in Kenya. The NIIMS is intended to work with the Integrated Population Registration System, to enable the linking of the central database with other functional identity systems within Kenya. In February 2020, the High Court of Kenya delivered a judgment ("*Huduma Judgment*") on the constitutional validity of the NIIMS.

RULE OF LAW TESTS

1.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The National Integrated Identity Management System, also known as Huduma Namba scheme, has been established under section 9A of the Registration of Persons Act of 1949. Alongside, the Integrated Population Registration System has been established under Kenya Citizens and Foreign Nationals Management Service Act (2011). Both the Registration of Persons Act and the Kenya Citizens and Foreign Nationals Management Service Act are acts of the Kenyan Parliament.

However, the amendments made to the Registration of Persons Act was challenged before the Kenyan High Court as being promulgated in a form that was not accessible. They were promulgated in a Miscellaneous Amendments Bill, which came into force on January 18, 2019 as Statute Law (Miscellaneous Amendments) Act No. 18 of 2018.¹ The Act is 86 pages long and contains provisions modifying more than fifty laws, and a petition challenging the NIIMS before the Kenyan court claims this was an obfuscatory tactic.

The use of a miscellaneous amendments bill to pass substantive amendments does not pass muster against the 'quality of law' requirement in our Evaluation Framework. Miscellaneous amendments must only contain minor, non-controversial amendments. The Huduma Bill, 2019, which intended to govern the NIIMS is yet to be passed, and is currently in the stage of public consultation.

In the absence of a legislative framework governing the NIIMS, we will look at the provisions in the proposed legislation, the Huduma Bill, 2019, in this case study to understand the intended governance of the NIIMS system.

¹ Khusoko, "Kenyan High Court Begins Hearing on Huduma Number," Khusoko, September 2019. <https://khusoko.com/2019/09/23/kenyan-high-court-begins-hearing-on-huduma-number/>.

1.2 LEGITIMATE AIM

Does the law have a legitimate aim? Does the law clearly define the purposes for which the ID can be used?

The primary requirement of the legitimate aim test is that the actions in questions must respond to a pressing social need, and should not operate in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

The objectives laid down in the Huduma Bill, 2019 to — promotion of efficient delivery of public services, consolidation and harmonisation of the law on registration of persons, facilitation of assigning of Huduma Namba and issuance of identity documents satisfy the legitimate aims test.

1.3 DEFINING ACTORS

Does the law governing digital ID clearly define all the actors that can use/manage or are connected to the ID database in any way?

The Huduma Bill clearly states that upon setting up of the NIIMS database, every government agency shall authenticate foundational data they hold of an individual with the NIIMS database.² It also states that every government agency delivering a public service shall be linked to the NIIMS database in such manner as to enable such agency to — (a) authenticate personal data in their possession with NIIMS; and (b) transmit, access or retrieve information necessary for the proper discharge of agency's functions. The Huduma Namba is clearly intended to serve as a foundational and single identity system to which all other government databases shall be linked.

It is not clear in the proposed law whether private parties can also use the Huduma Namba.

² Section 17, Huduma Bill, 2019.

1.4 REGULATING PRIVATE ACTORS

Is the use of the ID system by private actors adequately regulated? Are private actors held to the same level of accountability?

As mentioned above, the proposed law does not provide any clarity on the use of Huduma Namba by private actors, and is silent on their regulation.

1.5 DATA SPECIFICATION

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

The Huduma Bill defines a set of foundational data that will be collected for all persons enrolling under it.

The description of biometric data to be collected is not specific as it states 'fingerprints and any other biometric data.'

If the primary purpose of biometric data is verification and/or authentication, there are no clear grounds expanding the scope beyond fingerprints.³ Further, the Bill also mandates collection of functional data,⁴ which is defined as data for an individual created in response to a demand of a particular service or transaction.⁵ This is extremely vague, and it is unclear why there is a need for a centralised databases of functional data.

The *Huduma Judgment* holds that collection of biometric data for the purposes of identification was valid, however the storage and processing of biometric data without an implemented data protection legislation was unconstitutional.⁶

³ Section 2, Huduma Bill, 2019.

⁴ Section 6, Huduma Bill, 2019.

⁵ Section 2, Huduma Bill, 2019.

⁶ *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.

The Bill indicates that purpose limitation will be followed in Section 11, but the purposes for the data collected is not clearly defined.

1.6 USER NOTIFICATION

Does the ID system provide adequate user notification mechanisms?

There are no clearly defined requirements for notification to the individuals concerned in the case of access by third parties.

There are provisions in place to provide notifications in case of unauthorised access “within a reasonably practicable period of becoming aware of such breach.” The Bill also states that communication of a breach to the data subject may not be required where appropriate security safeguards such as encryption of affected personal data have been implemented.⁷ However, even under such circumstances, it is necessary that notification is done.

The Data Protection Act, 2019, in Section 43, requires the data controller to notify the Data Commissioner and data subjects of any unauthorised access to their data where there is a real risk of harm to the data subject. However, as the office of Data Commissioner is yet to be created, this measure is ineffective in addressing any breaches currently.

1.7 USER RIGHTS

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

Currently, there are no clear rights enshrined in the Registration of Persons Act.

Section 26 of the Data Protection Act, 2019 provides for rights to confirmation, access, correction, objection and deletion. However, as the Data Protection Authority has not been created yet, it is unclear how individuals can seek redressal.

⁷ Section 43, Huduma Bill, 2019.

The Bill provides individuals the rights to access, correct and object to use of their data. While the Bill provides the individuals the right to be informed of the use to which their personal data collected is to be put,⁸ it does not provide the right to know which individuals or entities can access their data.

There are no rights to opt out or deletion of data in the NIIMS database.

1.8 REDRESSAL MECHANISMS

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

The Huduma Bill has limited provisions on redressal mechanisms to deal with violation of rights. It only has an enabling provision under which complaint procedure would be created, but such mechanisms are not defined in the legislation itself.⁹

The redressal mechanisms under the proposed Huduma Bill are extremely inadequate.

The Data Protection Act has certain redressal measures for violations: Section 56 allows aggrieved data subjects to lodge a complaint with the Data Commissioner, who has the powers to investigate the offence,¹⁰ and enforce penalties.¹¹ Appeals from the Data Commissioner's action can be brought to the High Court of Kenya.¹² Data subjects are also entitled to compensation for damage caused by actions of data controller or processor.¹³

⁸ Section 36, Huduma Bill, 2019.

⁹ Section 58, Huduma Bill, 2019.

¹⁰ Section 57, Data Protection Act, 2019.

¹¹ Sections 58–62, Data Protection Act, 2019.

¹² Section 64, Data Protection Act, 2019.

¹³ Section 65, Data Protection Act, 2019.

1.9 ACCOUNTABILITY

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

The NIIMS system is intended to be governed by NIIMS Coordination Committee led by the Principal Secretary to the Home Department in Kenya.

The proposed Huduma Bill does not envisage an independent regulator.

The administrators are not made responsible for any breach of the system. In fact there are no provisions in the Bill to ensure accountability from the NIIMS Coordination Committee. The Principal Secretary is authorized to establish mechanisms for lodging complaints and facilitating amicable and expeditious settlement of disputes by any person aggrieved by any decision under the Bill.¹⁴ This poses a conflict of interest as adjudicatory powers are being delegated or discharged by bodies which may be subject to the same adjudication.

1.10 MISSION CREEP

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

The purposes for which Huduma Namba may be used are not clearly specified in the proposed Huduma Bill.

It is also not made clear which are the categories of actors who may make use of it. However, the Bill does provide a list of mandatory uses of Huduma Namba¹⁵ which are indicative, but is silent on other voluntary uses.

However, the Kenyan High Court in the *Huduma Judgment* held that purpose limitation was in built in the legal design of NIIMS and that the purposes are identification and verification. This does not serve as effective purpose limitation as identification and verification are features of the ID system itself and would be

¹⁴ Section 58, Huduma Bill, 2019.

¹⁵ Section 8, Huduma Bill, 2019.

part of *any* use of the ID. Without codifying specific instances or uses for which the ID system may be leveraged, the governing law has failed the purpose test.

1.11 NEWER PURPOSES

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

There are no provisions in place or practices envisaged to have a process for determining the appropriateness or legitimacy of new uses and purposes.

Even for mandatory uses, the provisions of Huduma Bill state that any other purposes for public service may be specified but this is not made clear. It is unclear how this will be impacted by the Huduma Judgment which clearly identifies identification and verification and purposes of the NIIMS. Additionally, the Huduma Bill clearly states that upon setting up of the NIIMS database, every government agency shall authenticate foundational data they hold of an individual with the NIIMS database.¹⁶ It also states that every government agency delivering a public service shall be linked to the NIIMS database in such manner as to enable such agency to – (a) authenticate personal data in their possession with NIIMS; and (b) transmit, access or retrieve information necessary for the proper discharge of agency's functions. This suggests an expanded scope of an unspecified number of actors using the personal data being collected.

¹⁶ Section 17, Huduma Bill, 2019.

RIGHTS BASED TESTS

2.1 DATA MINIMISATION

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

The Registration of Persons Act does not address data minimisation concerns.

The principles of data minimisation are also not discussed or clearly reflected in the proposed Huduma Bill.

The Bill envisages centralised collection of unspecified functional data.¹⁷ However it does not provide any principles on how the collection, use and retention of such data can be minimised. The Bill does refer to principles of purpose limitation in that the purposes for which data is collected will be specified to individuals, and that the individual consent shall be sought for further sharing of data with third parties.¹⁸

2.2 ACCESS TO DATA

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

Currently there are no laws that govern access of private and public actors.

The proposed Huduma Bill provides an expansive list of mandatory uses, which gives an indication of public bodies which may use it.¹⁹

It is not clear whether the agencies in charge of these functions may get access to any information collected. The Huduma Bill is silent on the access or use that private parties may have to the data collected.

¹⁷ Section 6, Huduma Bill, 2019.

¹⁸ Section 11, Huduma Bill, 2019.

¹⁹ Section 8, Huduma Bill, 2019.

It was argued in the Huduma Namba case that the NIIMS' legal framework was open-ended and did not specify the uses that it would be put to. On this question, however the court said that purpose limitation was a part of the legal framework and that the purpose of data collection was identification and verification of individuals. It is not clear whether this means that the data collected can only be used for the purpose of verification.

2.3 EXCLUSIONS DUE TO DESIGN FLAWS

Is the use of digital ID to access services exclusionary?

The Registration of Persons Act does not have any clear provisions on exclusionary impact and how to address it.

The Huduma Bill authorizes the development of measures to mitigate on any legal, procedural and social barriers that may limit enrolment, with special attention being paid to any group or persons at risk of exclusion. However, despite the provisions in Section 60, the Bill does not sufficiently address the challenges faced by marginalised communities such as Somalis and Nubians as well as Kenyan women, during the registration of persons.

This is one of the main arguments made by the petitioners in the lawsuit currently pending against the NIIMS system. However, in the Huduma Judgment, the Kenyan High Court did not provide a finding on the question whether making enrolment into NIIMS mandatory in order to access entitlements or services would be unlawful. Currently there are no clear provisions that mandate the use of the *Huduma Namba* to access services and entitlements and therefore, the Kenyan High court may not have felt the need to rule conclusively on this point yet.

2.4 EXCLUSIONS DUE TO FAILURE

Does failure of the ID system lead to exclusion?

In our desk research we did not come across clear account of exclusions arising as a result of the use of the digital identity. However, according to the Kenya National Electrification Strategy, the country will be fully electrified by 2022. It is also estimated that about 90% of the population of Kenya live within range of a

mobile tower.²⁰ These factors do mean that those without electricity and mobile connectivity will suffer exclusionary effects of digital identity.

The lack of clear alternatives to the Huduma Namba scheme suggests that exclusion will remain a concern.

Additionally, there are no clear provisions addressing exclusions arising out of incorrect data collection in the Bill.

²⁰ World Bank, “Kenya Launches Ambitious Plan to Provide Electricity to All Citizens by 2022”, World Bank, December 06, 2018, <https://www.worldbank.org/en/news/press-release/2018/12/06/kenya-launches-ambitious-plan-to-provide-electricity-to-all-citizens-by-2022>.

RISK BASED TESTS

3.1 RISK ASSESSMENT

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

There is no clear consideration of risk based factors in the proposed Huduma Bill.

While Section 60 of the Bill seeks to address exclusionary risks of Huduma Namba and states that the Cabinet Secretary shall develop measures to mitigate on any legal, procedural, and social barriers that may limit the enrolment, with special attention being paid to any group of persons at risk of exclusion for cultural, political or other reasons, at the moment there is no clarity on what these measures could be.

3.2 PRIVACY RISK MITIGATION

Is there a national data protection law in place?

During the pendency of the Huduma Namba case, the Kenyan parliament passed the Data Protection Act. The Kenyan High Court noted that the provisions of this law were in line with internationally recognised best practices, however without the implementation of the provisions of the legislation, the Huduma Namba project should not move forward. For this, a Data Protection Authority needs to be established under the Data Protection Act.

As the Kenyan High Court itself noted in the Huduma Judgment, currently the national data protection law has not been implemented in Kenya.

3.3 PRIVACY BY DESIGN

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

There are no clearly identified privacy by design strategies to minimise the harms of data breach.

3.4 RESPONSE TO RISKS

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

The legislative framework does not envisage any clear mitigation strategies in case of failure or breach of the ID system.