Case Study: Deploying Digital Identity Systems

Human Rights Implications and Lived Experiences in Kenya

Researcher: Sigi Waigumo Mwanzia

PARADIGM INITIATIVE

Credits

Principal Author:
Sigi Waigumo Mwanzia

Editorial Support:
Adeboye Adegoke, Senior Program Manager, Paradigm Initiative.
Ekai Nabenyo, Programs Officer (East Africa), Paradigm Initiative.

Supported by Omidyar Network

Design and Layout:
Kenneth Oyeniyi, Communications Assistant, Paradigm Initiative.

Find us online:

@ParadigmHQ

media@paradigmhq.org

PARADIGM INITIATIVE

HQ: 374 Borno Way, Yaba, Lagos - Nigeria.

Table of Contents

Introduction

The ability to legally 'prove who you are' continues to dominate regional and international public discussions, following governments' increasing attempts to capture, digitise and harmonise identification data into digital identity (ID) systems. Depending on country context, governments typically deploy these systems to either create a 'universal foundational scheme' or 'harmonise multiple functional systems' to facilitate proof of legal identity for various purposes, including identification, authentication and/or verification.

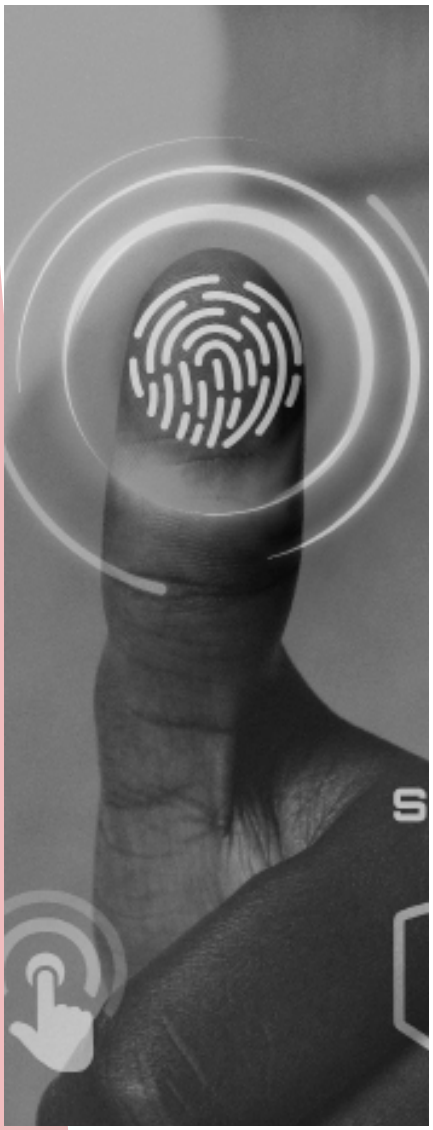
Ongoing public discussions focus on two mutually-reinforcing arguments highlighting the societal benefits and the potential for misuse of digital ID systems. On one hand, stakeholders, including governments, private sector entities and the international community, maintain that digital ID systems are a necessary 'public good' and crucial for the modernisation and efficient delivery of public services. The uptake of this narrative by governments is captured in national development and digitisation blueprints. It is also argued that "good" digital ID systems facilitate the Sustainable Development Goals, which call for legal identity to be provided to those who are legally 'invisible' by 2030.

On the other hand, stakeholders, including human rights organisations, document the human rights and lived implications of digital ID systems. Some of the cross-jurisdictional implications observed include, but are not limited to, challenges of poor participation in the law-making process, risks of exclusion for various individuals and minority communities without analogue identification documents, risks of mass and targeted surveillance and profiling using centralised databases, threats to privacy, data protection and transparency.

This case study documents the lived, rather than representative, experiences of two individuals between October and December 2020, after the deployment of Kenya's digital ID system. The individuals were selected with gender, geographical and community considerations in mind. The male informant identifies with the Kenyan Nubian community, and resides in Nairobi county, whereas the female informant identifies with the Somali ethnic group and operates in both Nairobi and Garissa counties. This primary research was supplemented with print and digital media information.

Kenya was selected due to its recent canvassing of the 'inclusion, security, and governance' issues, both in the 'court of public opinion' and the court of law. The lessons learned from Kenya's digital ID experience offers practical and comparative insights for other jurisdictions considering the deployment of digital ID systems.

Key Digital ID Terms: Definitions



Digital ID is a contested term but generally means a unique, electronic representation of an individual online. An individual's digital ID typically serves various functions, depending on the purpose (i.e., functional or foundational), but typically enables identification and verification.

Legal identity means 'the basic characteristics of an individual's identity e.g. name, sex, place and date of birth.' Legal identity may be conferred either through birth registration or through civil registration, with both systems relying on recognition of status by a legally-authorised registration or identification authority. One's legal identity ceases upon registration of death.

Foundational ID systems refers to legal identity systems, including 'civil registers, national IDs and population registers, which are created to provide identification to the general population for a wide variety of transactions' and needs. In the Kenyan context, foundational data includes 'registration number; name (in full); sex; county of birth; or country of residence; date of birth or apparent age, and place of birth; occupation, profession, trade or employment; place of residence and postal address, Global Positioning Systems coordinates, Land Reference Number, Plot Number or House Number, if any; finger and thumb impressions but in case of missing fingers and thumbs, palm or toe or palm and toe impressions in physical form; biometric data; date of registration; such other particulars as may be prescribed.'

Functional ID systems refer to 'identification, authentication and authorisation' systems used for 'specific sectors or use-cases.' These include, but are not limited to, tax, voting, electoral, health insurance systems.

Kenya's Digital ID System: Amending the Registration of Persons Act

"*There is an enemy called the file which we are trying to get rid of in public service. The days of lost files, long queues and wastage of time instead of providing efficient service to citizens will be a thing of the past*," Cabinet Secretary (**CS**) for the Ministry of Interior and Coordination of National Security in Kenya, CS. Fred Matiang'i.

Kenya's digital ID system, the National Integrated Identity Management System (**NIIMS)** was established following amendments to the Registration of Persons Act (CAP 107). These amendments were effected using an omnibus framework, the Statute Law (Miscellaneous Amendment) Act (No. 18 of 2018) (**Statute Law establishing the NIIMS**). This omnibus framework received presidential assent on 31 December 2018 and commenced operation shortly thereafter on 18 January 2019.

The NIIMS is a centralised 'national population register' and acts as a 'single and primary source of personal information and foundational data' of all Kenyan citizens and registered foreigners' resident in Kenya. This national population register is three-tiered and consists of a 'NIIMS database, a Huduma Namba, and a Huduma Card' (Rule 5, Registration of Persons (National Integrated Identity Management System) Rules (NIIMS Rules), 2020).

The NIIMS database, an integrated digital population register, operates the primary source of foundational data, and captures both foundational and functional data. The functional data referenced here includes data 'generated and linked by any agency responsible for a function requiring the use of the Huduma Namba.' The data captured in the NIIMS database will exclusively be used to assign the Huduma Namba - a 'unique and permanent personal identification number', issue the Huduma card and passports, and support the access and issuance of electronically generated copies of identity documents. The NIIMS database is also expected to facilitate the use of biometric data for identification purposes (Rule 6 (a), NIIMS Rules, 2020).

Under the NIIMS, refugees, minors above the age of six years, citizen adults and foreign nationals will only be able to prove their identity by presenting either the Huduma Namba or the Huduma Card. This proof of identity must be authenticated using biometrics.

Concerningly, the definition of biometric and biometric data in the Registration of Persons Act and the Data Protection Act, 2019 are not compatible. This may result in a different application of the terms by the Office of the Data Commissioner (**ODPC**) and the Ministry of Interior. These differing terms do not promote clarity and legal certainty for both enforcers of the law and those who are expected to abide with the two laws.

Instructively, Section 3 of the Registration of Persons Act defines biometric as 'unique identifiers or attributes including *fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form*' (emphasis added). Conversely, Section 2 of the Data Protection Act, 2019 defines **biometric data as** 'personal data resulting from specific technical processing based on *physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition*' (emphasis added).

Digital ID on Trial: Contesting the Deployment of NIIMS

Kenya's digital ID system with threatens fundamental rights and freedoms under the Constitution of Kenya, 2010. In February 2019, three human rights organisations (**petitioners)** challenged the deployment of the NIIMS by the Kenyan government. The petitioners include the Nubian Rights Forum, the Kenya Human Rights Commission, and the Kenya National Commission on Human Rights. has been

The petitioners raised three substantive human rights challenges. These included: -

a. the constitutionality of the legislative process which led to the enactment of the Statute Law establishing the NIIMS;
    i. whether the Statute Law establishing the NIIMS was subjected to public participation as enshrined under the Constitution;
    ii. whether the enactment of the Statute Law establishing the NIIMS using an omnibus framework was procedural or appropriate
    iii. whether the Statute Law establishing the NIIMS was a Bill concerning counties and should therefore have been subjected to approval of the Senate.
b. the impact (violation or threat) and limitation on the right to privacy and data protection under Article 31, Constitution of Kenya, 2010; and
    i. whether the collection of personal information under the NIIMS is intrusive, excessive and disproportionate;
    ii. whether the rights of children to privacy are violated or threatened by the NIIMS;
    iii. whether the personal information collected under the NIIMS has sufficient legal and data protection safeguards.
c. the impact (violation or threat) on the right of equality and freedom from discrimination under Article 27 of the Constitution of Kenya, 2010 and the impact on the Nubian community, and other marginalised communities.

The petitioners also filed applications for conservatory orders, i.e., temporary orders to safeguard the rights of a party/parties pending the final determination of a dispute. These sought to prohibit the government from implementing the new provisions under the amended Registration of Persons Act, implementing the registration of the NIIMS, and restraining the government from transferring or selling all data collected for the registry, in line with international best practice.

In April 2019, the High Court issued interim orders which coincided with the first 'Huduma Namba' mass registration process, which ended on 25 May 2019. These orders permitted the government to proceed with the mass registration, albeit with various restrictions. Here, the court prohibited the government from 'compelling' individuals or communities to participate in the collection of personal information and data in NIIMS. This order affirmed that **registration would proceed as a voluntary, rather than mandatory, process**.

Building on this, the court prevented the government from imposing 'time restrictions or deadlines' for the collection of personal information, and linking registration to one's ability to access public services or facilities. Further, the court also prevented the government from sharing or disseminating personal data collected in NIIMS to any person, including national and international governments and non-governmental agencies.

Between May and December 2019, reports indicated that a second mass registration drive would be conducted, but this did not happen. In January 2020, a three-judge bench permitted the Kenyan government to continue implementing the NIIMS, subject to various restrictions (**NIIMS decision**). Crucially, the government was tasked with enacting an 'appropriate and comprehensive regulatory framework' which complied with the Constitution of Kenya. Additionally, the High Court invalidated the provisions in the amended Registration of Persons Act which enabled the Government to collect DNA data and GPS coordinates for identification purposes. Here, the Court held that these provisions violate the right to privacy under Article 31 of the Constitution of Kenya, 2010. The Court also maintained that the collection of this sensitive personal data required the prior enactment of 'empowering legislation.'

The petitioners disagreed with the Court's judgment and lodged an appeal before the Court of Appeal. A determination of the same is yet to be made.

Lived Experiences

The insights obtained from in-depth interviews with two individuals (informants/ interviewee's) illustrate their lived, rather than representative, experiences during the deployment of Kenya's digital ID system. These experiences cannot be extended to the two ethnic groups or the larger Kenyan population, but each individuals' experience offers critical insights into some generally acknowledged risks of digital ID systems.

These two individuals have interacted with the system in varied capacities, including as members of different gender, geographical and community groups. The female informant identified as belonging to the Somali ethnic group, operating and residing in both Nairobi and Garissa counties, and had registered for the Huduma Namba. The male informant identified as belonging to the Nubian community residing in Nairobi county and had not registered, deliberately, for the Huduma Namba.

Insight 1: Patching Due Process - Legitimising the NIIMS

Out of the two individuals we spoke to, one individual expressed their discomfort with the High Court's judgment and noted that the digital ID system was 'rolled out without a proper law.' Restrictions on due process and good governance impact political, socio-economic and cultural rights, including the right to political expression through public participation.

Kenya's digital ID system neatly epitomises the phrase 'placing the proverbial cart (*NIIMS*) before the proverbial horse (*due process and the rule of law*).' In 2020, Paradigm Initiative documented the concerns by Kenyan stakeholders following the government's failure to provide adequate, participatory and stand-alone digital ID and data protection laws. As one informant noted, the government attempted to follow due process, '[only] after we went to Court.'

These failures gave rise to a patch-work of measures at the government level to address constitutional and due process violations. To legitimise the NIIMS, various laws, regulations and rules were either prepared or implemented *after* the digital ID system had been deployed. These include various iterations of the draft Huduma Bill, which was released for public consultation in July 2019 but still remain at the Cabinet and NIIMS Committee levels. Shortly thereafter, Kenya's Data Protection Act, 2019 (**DPA, 2019**) was assented on 8 November 2019 and commenced operation on 25 November 2019. In October 2020, 10 months after the court decision on the NIIMS, two NIIMS regulatory frameworks, including the NIIMS Rules, were gazetted.

This legitimisation process is still a core concern for stakeholders who question the procedural and substantive legality of the Statute Law establishing NIIMS, despite the NIIMS decision. In October 2020, the High Court validated one claim of procedural irregularity affecting the Statute Law establishing NIMS, namely the procedure of determining if a Bill concerns county governments.

Notably, 23 Acts, including the Statute Law, were nullified due to failures by the speakers of the National Assembly and the Senate to concur as to whether a bill concerns counties,

prior to a Bill being introduced before either house, in contravention of the Constitution of Kenya. The judges in the NIIMS decision refused to deal with this issue on grounds that the Petitioners' failed to raise this issue 'in their pleadings.' Despite the significance of this nullification, this order was suspended by the Court for a nine month period, permitting the two Houses of Parliament to rectify this due process (procedural) issue.

Insight 2: Weakened Agency during Registration - Misleading Government Claims and Community Norms

"*National ID Card is an identification document issued under Section 9 of Registration of Persons Act. The Act has not been repealed or amended to enable substitution of ID Cards with Huduma Cards... as directed by CS Mucheru. The directive is unlawful. ^POLSK*," President of the Law Society of Kenya, Mr. Nelson Havi.

Out of the two interviewee's, only one individual registered during the mass registration process in 2019. The second individual did not register because he was directly involved in the constitutional petition 'challenging the government on Huduma Namba.'

During the first mass registration process, reports by the media and other stakeholders confirmed that the government had contravened the Court's interim directives, with the 'President of Kenya leading misleading claims by government officials.' Notably, the government imposed 'time restrictions and deadlines' for this registration process, from April to May 2019, and further mandated registration, prior to accessing government services.

In April, the Communications Authority of Kenya's Director General cautioned individuals who failed to register for Huduma Namba that their SIM cards would be blocked, resulting in restricted or inaccessible mobile phone access. During the same month, the media reported that the Machakos County administration, a county in the Eastern part of Kenya, notified government employees that their salaries would be withheld, if they failed to register for Huduma Namba.

One informant noted that individuals resident in Kenya 'were threatened to register [and participated] out of fear and not because they understand what NIIMS is, or its purposes.' These threats and the poor understanding of the challenges NIIMS seeks to address, persist to date. In November 2020, the CS, Ministry of ICT claimed that the Huduma Namba card will replace Kenya's national ID card by December 2021, failing which individuals will be unable to gain access to essential public services. This claim has raised further questions, including from the President of the Law Society of Kenya, about the legality of these government initiatives, noting that this substitution has not been provided for under law.

The informant who registered confirmed that the government was conducting door-to-door registration in peoples' homes. This was replicated across the whole country in offices, malls, schools, churches, marketplaces, and estates. During the registration by Huduma Namba officials, the informant confirmed that she 'didn't want to register at first but the people who were registering came home and they registered my parents and

siblings, so I also participated.' While this individual was not compelled to participate in the registration process, her experience indicates that some individuals felt pressured to register to fit in with family and community norms, rather than exercise agency based on informed consent.

Insight 3: Registration Barriers and Risk of Exclusion for Minority Groups and Individuals

The High Court affirmed, in its 2020 judgment, that 'there may be a segment of the population who run the risk of exclusion.' Based on the lessons learned from the primary and secondary research, pre-existing and unresolved registration barriers before the deployment of the NIIMS in Kenya heightened exclusion risks for various groups. These includes individuals and communities without identity documents, people with biometric challenges (e.g., unreadable fingerprints), women, persons with disabilities and double-registered individuals.

Insight 3.1: Identification Document Challenges

"There are many challenges if you don't have an ID...If you want to open up a bank account, you need an ID. If you want to see someone in court, you will be asked for an ID. In Kenya, you cannot go anywhere without an ID," Amina Ali Adan.

Both informants confirmed that individuals had to present their 'national ID (for adults) or their birth certificate (for minors)' before they could be registered for the NIIMS. Notably, the government Spokesman reportedly acknowledged that many of the people who were unable to register in 2019 'did not have national Identification Cards and birth certificates by the time the drive was completed,' necessitating the government to provide a 'grace period' between registration processes.

The next mass registration process is reportedly set to commence in April or May 2021. However, stakeholders criticise the government for availing a short grace period during which ID card and birth registration coverage was not simultaneously expanded.

The interview from Somali ethnic group noted that her decision to register during the door-to-door registration was informed by contextual realities affecting the identification process in Garissa sub-county. Here, the interviewee drew upon her experiences of the analogue registration process for a national ID in Garissa sub-county, and noted that individuals 'only have one chance to apply for an ID, and if you miss this window... sometimes [you] have to wait until the next year to apply.'

In Garissa sub-county, women are more prone to exclusion owing to systemic failures to provide the entire population with ID documents. One informant confirmed that 'women in Garissa County likely faced more challenges than men' during the registration process. The informant confirmed that women who have attained the age of 18 are 'often asked to come with their parents to place their fingerprints' in order to obtain a national ID. Here, the informant noted that this arrangement often proves difficult because 'most of these communities are pastoralist, frequently travel, and may not be able to present themselves physically' during the available registration opportunity (once a year).

Further, this individual drew upon her work experiences and confirmed that registration barriers exist for double registered individuals in Kenya, i.e., Kenyan citizens who are registered in the biometric refugee database. These individuals, according to the informant, are 'unable to obtain ID documents, and have to undergo lengthy vetting processes [which are often affected by] errors and delays.'. The interviewees also acknowledged that a 'large number of Nubians do not have an ID or a birth certificate' due to the vetting challenges which also affect the Nubian community.

Concerningly, Kenya's digital ID framework does not adequately cater for persons with disabilities, and neither the draft Huduma Bill nor the NIIMS Rules, 2020 have addressed this exclusion.

Insight 3.2: Registration Anomaly

Curiously, the informant from the Nubian community noted that some members managed to register for Huduma Namba, including those 'without an ID or a birth certificate.' The male informant pointed out that the government 'played games' during the mass registration exercise, and deliberately registered some Nubians to demonstrate that the system does not promote exclusion or discrimination. However, this ability to register without an identifying document was not applied uniformly across the board, which resulted in 'some people [being] chased away when they tried to register.'

Insight 4: Privacy, Data Protection and Surveillance Concerns

Insight 4.1: Lack of Independent Oversight

During the interviews, both interviewee's expressed concerns about the protection of personal information under the NIIMS, and commented that they 'don't know how the government will misuse this information, and you know the government of Kenya.' One informant noted that the data capture form (Form HN 1) contained 'very personal questions,' including those on land ownership, which she was uneasy responding to. However, both informants were optimistic that the DPA, 2019 may be able to respond to the misuse risk.

The DPA, 2019 was operationalised nearly 10 months after the NIIMS was established. This gap permitted both state and non-state actors to collect personal data during mass registration processes without independent oversight. Instructively, the government had already finished the data clean up and merging process and issued the first batch of Huduma Namba cards following the first registration process before Kenya's first Data Commissioner was sworn in in November 2020.

Despite the operationalisation of the Office of the Data Protection Commissioner (**ODPC**), the challenge of independent oversight has not been addressed. Here, Kenya's ODPC functions as a state office within the ICT Ministry, which is itself a data collector, rather than an independent authority.

Additionally, data protection and transparency are mutually-reinforcing concerns which facilitate the rights to freedom of expression and access to information. Problematically, the government has failed to clarify why the NIIMS needed to be established, given the existence of another population register, the Integrated Population Registration System (**IPRS**). The IPRS, which was rolled out in 2015, is also touted as a 'single source of truth' register and still plays a central role in Kenya's identity ecosystem.

On the procurement front, it was alleged that the government had negotiated a deal with MasterCard to link the Huduma Card (Huduma Kenya services) with the Huduma Namba under the NIIMS. Despite the government's clarification, the type of public-private partnerships which have been formed between the government and private sector

entities to deploy the NIIMS remains largely unknown. Notably, the High Court refrained from making any 'findings on the procurement of NIIMS.'

Insight 4.2: Biometric Data - Surveillance and Profiling Concerns

The NIIMS database relies heavily on centralised biometric data for identification and authentication. The processing of sensitive biometric data exposes individuals to profiling, mass or targeted surveillance, and data misuse or breach risks, consequently infringing on individuals' right to privacy.

The United Nations High Commissioner for Human Rights stressed that the principles of legality, proportionality and necessity under international human rights law must be satisfied, where biometric databases are being deployed. Here, the provision of safety and security safeguards, including encryption and anonymity protections, must be prioritised, at both the legal and the design stages to protect fundamental rights. In the NIIMS decision, the Court affirmed that the government's failure to provide an adequate and 'specific regulatory framework that governs the operations and security of NIIMS... poses a risk to the security of data that will be collected in NIIMS.'

The High Court in the NIIMS decision noted that the framing of the NIIMS purposes, including harmonisation of data from other databases in Government agencies relating to registration of persons, permits 'cooperation with other agencies.' The Ministry of Interior confirmed that the NIIMS will be used for purposes beyond population registration and will play a 'key role in national security (including security surveillance) and curbing crime.' The potential for biometric data in NIIMS to be used for other purposes (**mission/function creep**), including unlawful tracking and profiling, remains a major concern for stakeholders.

Conclusion

This case study explores the human rights implications of digital ID systems, relying on insights obtained from the lived experiences of two individuals following Kenya's deployment of the NIIMS.

These insights have cross-cutting relevance for stakeholders considering the deployment of similar digital ID systems. On the due process front, robust legislative and regulatory frameworks must be developed, in a participatory manner, and enacted prior to the deployment of a digital ID system. As noted above, the Kenyan government's prioritisation of the NIIMS before due process and the rule of law led to public uproar and triggered a protracted, and ongoing, judicial battle. Similarly, the failure to prioritise due process at the procedural levels resulted in a (suspended) nullification of the Statute Law establishing the NIIMS in October 2020.

On the registration front, one interviewee expressed her discontentment with the process, as well as her initial desire not to register, revealing instances of weakened agency. Further, the failure by the government to deploy a grace period to ensure that as many people as possible had obtained an identification document, pre-deployment of the NIIMS, resulted in many individuals being unable to register. In turn, these systemic challenges affected and excluded various groups, including individuals without identity documents, people with biometric challenges (e.g., unreadable fingerprints), women, persons with disabilities and double-registered individuals.

On the privacy, data protection and surveillance front, concerts about personal data being misused was a central concern for both interviewee's. Despite the operationalisation of the Data Protection Act, 2019, Kenya lacks independent oversight which fails to adequately protect the right to privacy. Further, the use of centralised biometric databases require adequate safety and security safeguards to be put in place at the legal and design stages to ensure that profiling and surveillance risks are mitigated.

Questions for discussion

1. Does your country have a digital ID system in place? What legislative and regulatory frameworks established it? If there are no law and regulations, how is due process and the rule of law protected and promoted by the government?
2. What do you know about the digital ID system in your country? Is this information publicly accessible?
3. What type of data does the digital ID system collect and is it linked to the access of public services?
4. What safeguards exist to protect individuals' personal information and mitigate misuse, breach, profiling and surveillance risks? If these safeguards exist, do they work in practice? If yes, please explain how.
5. What exclusion and discrimination risks do the 'legally invisible' face in your country? If a digital ID system has been deployed, was a grace period provided by the government for these individuals and communities to obtain identification documents? Why? Why not?
6. What other human rights challenges do individuals and communities in your country face when attempting to prove their identity?
7. Should governments stop implementing digital ID systems until their human rights implications are properly understood? How can we make governments listen to our requests?

HQ: 374 Borno Way, Yaba, Lagos - Nigeria.