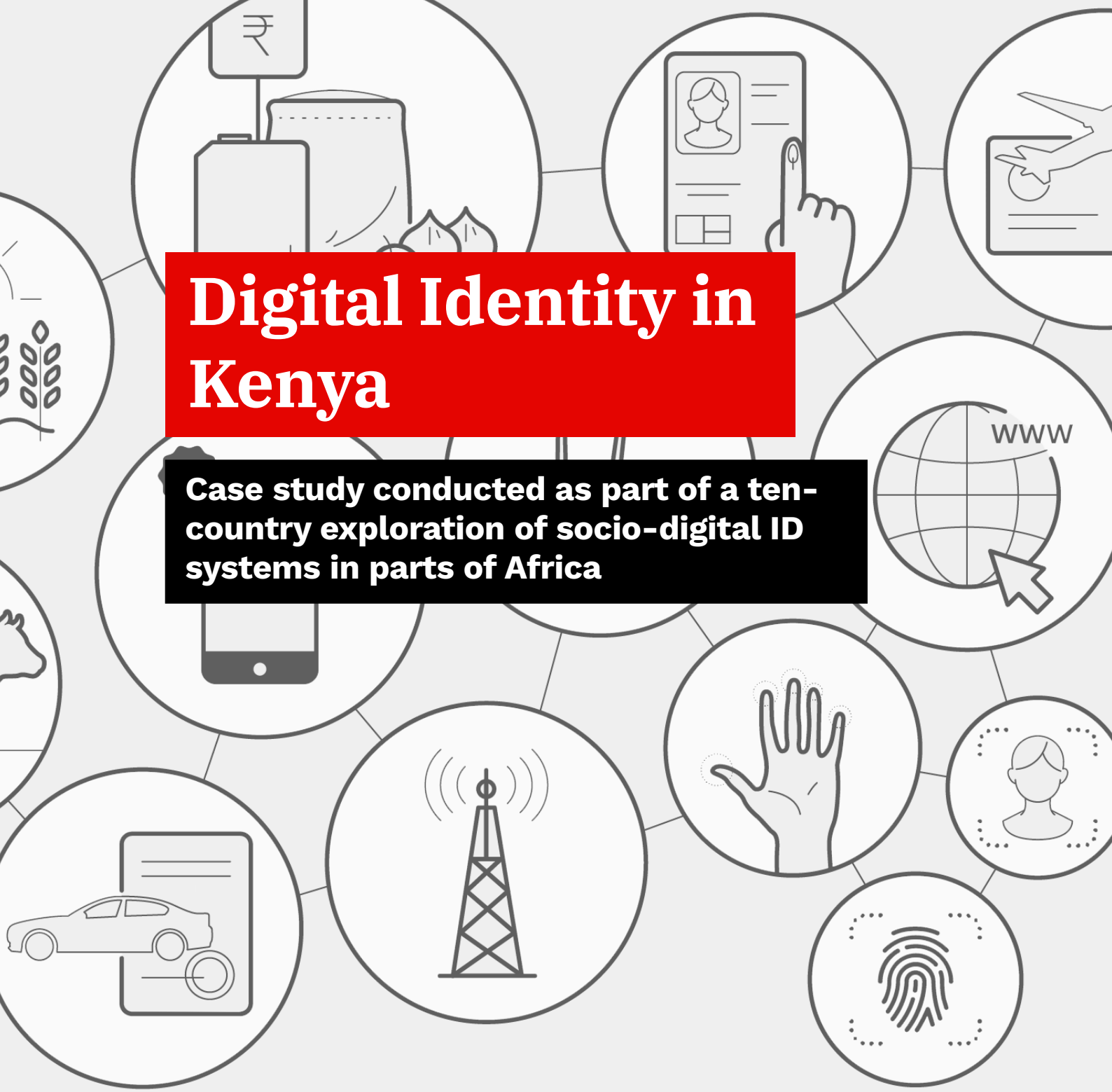

Digital Identity in Kenya

Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa

RESEARCH & WRITING
Grace Mutung'u

REVIEW & EDITING
Anri van der Spuy, Vrinda Bhandari, Shruti Trikanad & Yesha Tshering Paul

COPYEDITING
Samantha Perry

COVER ILLUSTRATION
Akash Sheshadri

LAYOUT
Aparna Chivukula

RESEARCH ICT AFRICA

THE CENTRE FOR internet & SOCIETY

OMIDYAR NETWORK™

Digital Identity in Kenya

Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa

A project of the Centre for Internet and Society (CIS), and Research ICT Africa (RIA)

→ digitalid.design ←
→ cis-india.org ←
→ researchictafrica.net ←

Digital Identity in Kenya

By Grace Mutung'u, Strathmore University

PREAMBLE

With an estimated 500 million people in Africa living without any form of legal identification (birth certificate or national ID),[1] the use of digital forms of identification has become increasingly popular because of their relative ease, low cost, and convenience compared to more analogue systems.

The Covid-19 pandemic has, if anything, increased the appetite for digital identification platforms and technologies.[2] The African Union Commission is currently working on a continental initiative to develop an interoperability framework for digital ID. Among other policy instruments, this effort draws its mandate from the *Digital Transformation Strategy* (DTS) *for Africa (2020-2030)*, which emphasises the importance of digitised legal identification mechanisms on the continent. The DTS highlights both the potential social and economic implications of digital IDs for Africans, noting that digital IDs not only support social development, but also enable meaningful participation in productive processes to generate economic growth, spur innovation, and support entrepreneurship. Besides being viewed as an enabler for realising all these policy objectives, digital IDs are seen as critical for the successful implementation of the African Continental Free Trade Area (AfCFTA).

With the growing enthusiasm for digital ID in Africa and across the world, there is a need to examine their impact on human rights, the rule of law, and the people who will be included (and excluded) from related systems. More critical analyses of digital ID's impacts in the global South, as well as the actors involved in designing and implementing them, are needed because digital identity programmes create an inherent power imbalance between the State and its people. The collection of personal data leave residents with little ability to exert

1 ID4D global dataset, 2018. See: *https://datacatalog.worldbank.org/dataset/identification-development-global-dataset*

2 Martin, Schoemaker, Weitzberg & Cheesman, 2021.

agency in its collection, storage and use, particularly when their right to privacy is not safeguarded or their personal data protected. And while increasing access to legal identification might appear to be a positive development for countries, this is not unequivocally the case.

In addition to the very real challenges of living without legal identification – whether digitised or analogue – those who *do* have digital do have digital identity may face other challenges. Experiences depend on (historical) context,[3] with some digital identities being developed in an attempt to segregate or even coerce people, while others are designed under the guise of national security concerns. Some countries have IDs that are no longer fit for purpose in a digital age,[4] while digitisation can also introduce novel harms. These include not only the direct risks associated with the collection and storage of personal data but arguably greater harms of exclusion or discrimination. Unless active measures are taken to counter such harms far from improving lives and potentially livelihoods, the introduction of digital ID systems could exacerbate inequality when analogue options are discarded – especially in African contexts with low connectivity levels.

On the other hand, digital identity systems, like all ICTs, are actively designed and shaped and therefore not inevitably detrimental from a developmental, human rights, and/or inclusion perspective.[5] If digital identities are conceived and designed with human rights, developmental goals, sustainability, and safety at the forefront, they might have a more transformative impact for the continent.[6] Critically examining the design, development, and implementation of these evolving systems remains crucial therefore, along with whether policymakers are doing enough (from a governance perspective) to ensure the positive outcomes of engagement with these socio-digital systems, while mitigating the risks that accompany many digital identities on the continent.

The Project

With this background in mind, Research ICT Africa (RIA) and the Centre for Internet and Society (CIS) partnered in 2020 and 2021 to investigate, map and report on aspects related to the state of digital identity in ten countries in Africa. The project looked at local (and digitised, in full or partially) foundational ID systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa,

3 Breckenridge, 2014.

4 African Union Commission, 2021.

5 e.g., Lievrouw, 2014; Parikka, 2012; Freedman, 2002; Wacjman, 2000; Williams, 1985.

6 c.f., Weitzberg, Cheesman, Martin, & Schoemaker, 2021.

Tanzania, Uganda, and Zimbabwe.

The research took place within parameters set by an Evaluation Framework for Digital Identities[7] (the 'Framework'), which was developed by CIS with the purpose of assessing the alignment of digital identity systems for compliance with international rights and data protection norms. (CIS initially developed the Framework with a view of using it to assess India's Aadhar system, but the Framework has since been used in other contexts too.)[8] By using this Framework, the ten country partners evaluated certain aspects of the existing governance and implementation mechanisms of digital identity in their respective and unique contexts.

The Framework introduces a series of questions against which digital identity may be tested, aiming to address the various rights and freedoms that are potentially impacted by the state use of a biometric digital identity program. More detail about the Framework can be found in Annex II.

This report on the Kenya case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Grace Mutung'u, Strathmore University. Besides being an independent case study, the findings from this report were also used to inform a comparative report put together by the RIA and CIS teams to analyse the similarities, differences, and other aspects across the ten case studies – including key recommendations for policymakers, researchers, civil society actors, and other stakeholders.

An important limitation of the research is that the country case studies were conducted using the analytical lenses provided by the Framework, partly with the aim of assessing whether the Framework is relevant in African contexts, and might therefore not cover all aspects pertaining to digital identity in the context concerned. We elaborate on this limitation – which we feel significant in the contextually rich and diverse African context – in the comparative report.

PREAMBLE REFERENCES

African Union Commission (2021). *Draft AU Interoperability Framework for Digital ID* (August, 2021). [not published.]

Breckenridge, K. (2014). *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge: Cambridge University Press.

7 *https://digitalid.design/evaluation-framework-02.html*

8 *https://digitalid.design/evaluation-framework-case-studies/estonia.html*, *https://digitalid.design/evaluation-framework-case-studies/kenya.html*

Freedman, D. (2002) *A 'Technological Idiot'? Raymond Williams and Communications Technology, Information, Communication & Society*, vol. 5(3): 425-442.

Lievrouw, L.A. (2014) "*Materiality and media in communication and technology studies: An unfinished project*." In: Gillespie, T., Boczkowski, P.J., Foot, K.A. (Eds.) (2014) Media technologies: Essays on communication, materiality and society. London: MIT Press.

Martin, A.; Schoemaker, E.; Weitzberg, K. & Cheesman, M. (2021) *Researching digital identity in time of crisis (workshop report).* London: The Alan Turing Institute. Available at: https://www.turing.ac.uk/sites/default/files/2021-08/3c_workshop_reporttimes_of_crisis_.pdf

Parikka, J. (2012) *New Materialism as Media Theory: Medianatures and Dirty Matter, Communication and Critical/Cultural Studies, vol. 9*(1): 95-100.

Weitzberg, K.; Cheesman, M.; Martin, A. & Schoemaker, E. (2021) *Between surveillance and recognition: Rethinking digital identity in aid. Big Data & Society*, January-June: 1-7.

Williams, R. (1985) *Towards 2000*. Harmondsworth: Penguin.

ACKNOWLEDGEMENTS

This report was made possible by the support received from Omidyar Network.

The Evaluation Framework referenced in this report was developed by the Centre for Internet and Society. The case study was conducted by Grace Mutung'u with the support of Research ICT Africa (Anri van der Spuy and Naila Govan-Vassen) and the Centre for Internet and Society (Shruti Trikanad, Vrinda Bhandari and Yesha Tshering Paul). The RIA and CIS teams do not necessarily agree with the views expressed in this country case study. The authors thank the people who made their time and expertise available to contribute to and review this report.

ABSTRACT

Like many other African countries, Kenya is implementing a digital ID programme. However, Kenya's digital ID comes with a lot of baggage, as it is an upgrade of its national identification document that has been in place since the colonial period. The national identity card is also a citizenship document that is required for movement within the country, access to buildings, access to government services such as education and health insurance, and access to private services such as employment and even for registration of a SIM card. Policy advocates therefore warn that moving to digital ID is not as easy as digitising the analogue register of persons, but will also involve solving issues of inclusion and belonging for communities that have had challenges accessing identification documentation over the last century.

In considering the challenges and opportunities of digitising an existing system such as Kenya's, the report finds that the main challenge with the legal framework is that it prioritises introduction of technology without resolving many other problems identified with the registration of persons law. Existing problems such as the discretionary powers of registration officers to issue the national identification card or lack of coherence between the Registration of Persons Act (RPA) and other citizenship laws persist. There are also concerns arising out of the National Registration Bureau - the office charged with registration of persons - being housed within the ministry of interior security. First, is the tendency to securitise registration of persons, where the lack of a national identification card is not only a criminal offence but presents an opportunity for a person to be harassed by law enforcement officers. Second, the police have appropriated for themselves a role in reputation management through practices such as issuance of police clearance certificates. Through this process, the police have normalised access to the national identification database, a practice that has greater implications in the digital age.

These problems could be solved through having a paradigm shift on identification documentation as a right as opposed to the current practices of securitisation. This can partly be achieved through a governing structure that is dedicated to resolution of citizenship and identification issues. The identification regime should also be more people-centric by providing opportunities for every person whose data is captured to not only have access to their data, but to also know who else has access to their data and for what reason. In view of the fact that the digital ID programme aims to create a population management database, the need for independent oversight for issues such as data sharing cannot be overemphasised.

ACRONYMS AND ABBREVIATIONS

CMCA	Computer Misuse and Cybercrimes Act
DCI	Directorate of Criminal Investigations
DPA	Data Protection Act
ICT	Information and Communications Act `
ID	Identity/ identities/identification
IPRS	Integrated Population Registry Services
KCFNMA	Kenya Citizens and Foreign Nationals Management Act
NIIMS	National Integrated Identity Management System
NRB	National Registration Bureau
RPA	Registration of Persons Act

CONTENTS

INTRODUCTION

1.1 THE CONTEXT

Kenya is among East Africa's most diverse countries, bringing together various cultures, languages and practises. Although the country is considered a regional economic powerhouse, inequality remains persistent. Over close to 60 years of independence from British colonial rule, the country has pursued different nation-building projects to enhance national cohesion and integration. These include a return to multiparty democracy in 1992 after years of a single party and, more recently, the enactment of the 2010 Constitution that guarantees a range of freedoms.

The Constitution's most distinguishing features include an expanded bill of rights and devolved government, both of which were meant to support the decentralisation of power and more equitable development. Citizenship was among the issues that were negotiated in the drafting of this Constitution. Consequently, there are elaborate provisions on citizenship, including guarantees on citizenship documentation for all Kenyans.

Citizenship documentation is an age-old concern in Kenya and is particularly contentious among border communities, minorities and non-white immigrants. Since independence, some of these communities have faced difficulties in acquiring national identity cards, including having to undergo additional administrative procedures to prove their descent. It was therefore expected that any new identity document would, following the constitutional provisions on citizenship, resolve issues of statelessness or the risk thereof. However, a new digital ID system introduced in 2019 made it mandatory to have a primary identification document (such as a national ID card or birth certificate in the case of children) to register for the digital ID system. The digital ID law was therefore contested at various fora, including through litigation.

In January 2020, the High Court of Nairobi issued judgement for consolidated petitions contesting Kenya's third generation identity cards, popularly known as *huduma namba*.[9] This was after civil society organisations the Nubian Rights Forum (NRF) and the Kenya Human Rights Commission (KHRC), together with the national human rights institution the Kenya National Commission on Human Rights (KNCHR), sought to halt the digital ID programme. The government put up

9 Swahili for "service number". The use of *huduma namba* is meant to shift the narrative from the current identity card's k*itambulisho* (Swahili for "identity"). *Huduma namba* indicates a change of concept from mere identity to delivery of services.

a spirited defence and two Principal Secretaries - the most senior technocrats in the ministries of ICT and interior - were called to testify. The country's privacy law, the Data Protection Act (2019), was also enacted during the case, referred here as NIIMS case/ judgement (Nubian Rights Forum and 2 others v Attorney-General and 6 others; Child Welfare Society and 8 others (Interested Parties), 2020; Data Protection Act, (No. 24 of 2019)).

Similarities can be drawn between the *huduma namba* contestations and similar concerns raised around 100 years before, when the British colonial government introduced fingerprinting of adult male Africans under the *kipande*[10] system, which required identification documents to be carried around the men's necks at all times, in a metal container suspended on a chain. The most obvious is the resistance to subjugation, in the 1920s to the colonial administration's *kipande*, and in 2020 through the government's collection of granular data.

Another similarity between the two systems is reputation management. In the 1920s, white employers kept records of their black workers in their identification documents (Weitzberg, 2020). A century later, the national identity card is the unique identifier in financial and criminal reputation management, through credit information sharing. As Breckenridge (2019) argues, private actors were a key driver for the digitalisation of identity systems in Kenya in the quest for a credit information sharing system. The government also maintains a criminal records database and it is common practice for government entities and private persons to ask prospective employees to get a police clearance certificate prior to employment. The certificate is obtained through running one's fingerprints against the criminal records database (DCI, no date). Many other parallels can be drawn from the importation of colonial methods of population management from colonies such as India and South Africa into Kenya, with surveillance philosophies that have traversed from private companies to the government (Breckenridge, 2014). As Kenya maintained the colonial systems, such as fingerprinting, the digital ID system aspires to digitise the analogue records and enhance the country's population database. An historical overview of the evolution of national identity provides some understanding of the factors that have influenced the current initiative for a digital ID system.

1.2 METHODOLOGY

This report uses the CIS framework to evaluate Kenya's digital ID system. The study primarily relied on desktop research, where cases, policies and reports on Kenya's digital ID programme were reviewed. This was complemented by expert interviews to clarify the status of issues referred to in resources, as well as

10 *Kipande* means 'piece' in Swahili, in reference to the identity certificate as a piece of paper and how it was worn as a neckpiece.

through observation at sites where government services are offered.

This research was conducted between March and June 2021. While the report was in the process of being proofread, a significant development took place when, in October 2021, the High Court ruled that the roll-out of *huduma namba* was illegal because a data protection impact assessment had not been conducted. In coming to this conclusion, the Court considered the implications of an earlier judgement in a case challenging the *huduma namba* project (NIIMS case) (examined in more detail later in this study). In the October 2021 judgment, the Court stated that the Data Protection Act would have been applied retrospectively, and that a data protection impact assessment should have been carried out prior to the roll-out of *huduma namba*. The Court therefore ordered the government to conduct a data protection impact assessment in accordance with Section 31 of the Data Protection Act before processing *huduma namba* data or rolling out *huduma* cards.[11]

1.3 OVERVIEW OF KENYA'S FOUNDATIONAL ID SYSTEM

Kenya has had systems for registration of persons since the beginning of the 20th century in the form of movement passes, birth registration and identification cards. The national identity system has been in force since 1920, when all African males over the age of 16 were required to register their details and have their fingerprints taken, after which an identity document known as *kipande* would be issued. This was governed by the Native Registration Ordinance of 1915. Following long resistance by Africans, the *kipande* was extended to all races under the Registration of Persons Act (RPA) in 1947. Upon independence in 1963, the government of Kenya inherited the system. It made minimum reforms, such as including women for registration in 1978 and raising the age of majority to 18 in 1980 (KNCHR, 2007, Chapter 2). The registration office was also transformed into a fully-fledged bureau under the ministry in charge of interior security. Otherwise, however, the *kipande* system remained intact in terms of data collected.

The *kipande* system records a person's identity, including ethnicity and clan. The ethnic definitions are based on the British view of African systems, and they erroneously categorise some clans, completely omit others and fail to account for fluidity of ethnicity (Khawaja, 2018; Mamdani, 2001).[12] There has been much

11 Read more about this development here: *http://kenyalaw.org/caselaw/cases/view/220495/*

12 For example, the colonial classification grouped a number of communities from Western Kenya as "Abaluhyia". However, as argued by Khawaja (2018), the classification was arbitrary, as the so called "Abaluhyia" dialects are dissimilar. The customs of these communities also vary significantly, raising questions on the basis for the colonial classification. Similar issues have also been raised about the "Kalenjin" classification for a number of communities found in the Rift Valley region as well as the initial classification of the "Kikuyu" people. For a general discussion, see Oucho, 2002.

debate about whether to maintain ethnic information in the register or not. Groups that face challenges in getting recognition from the government believe that listing them among the tribes of Kenya would increase their chances of getting not only identification documents but also government services. Ethnic data is also used in regional balancing for public offices (Balaton-Chrimes, 2021). However, ethnicity has also been used for political mobilisation, with dangerous results as witnessed in recent elections (NCIC, 2016). A 2018 amendment to the RPA does away with the requirement to declare one's ethnicity during registration, though the effect of this requirement is yet to be felt. At the time of writing this report, applicants for the national identity card were still required to declare their ethnicity.

The identity document itself initially consisted of papers placed in a piece of metal worn around the neck (*kipande*). In 1947, it evolved to a passbook that contained fingerprints and the portrait of the bearer. In 1980, it was reduced to a card containing the bearer's portrait and fingerprints. In 1995, a smaller bank card-sized typed and laminated card, known as a "second-generation card" and referred to as *kitambulisho*[13] was introduced. It contains the bearer's demographic information, a photo, a signature and an image of one fingerprint. There have been several attempts to introduce a third-generation identity card with better security as well as smart features. Since 2011, the identity card has been upgraded to a plastic card (Atellah, 2020).

In 2010, Kenya promulgated a new constitution with progressive provisions that were meant to address historical challenges for Kenya's national identity (Ng'weno & Aloo, 2019). Among the issues canvassed during the constitution-drafting process were citizenship and identity documentation (Nalule, 2020). The citizenship law was revised, and a new body - the Kenya Citizens and Foreign Nationals Service - was set up to harmonise matters of citizenship documentation. The service developed an integrated population register (IPRS) which has, since 2016, supported various e-government services. It has also been used by private parties such as banks, mobile network operators and insurance companies for the verification of identity documents (Kenya Citizens and Foreign Nationals Management Service (Charges for Use of Information from the Register) Regulations, 2016).

In a technical assessment of the country's identity systems, the World Bank commended Kenya for its advanced identity systems, which include civil registries and the national ID. The Bank recommended that the country integrate its multiple identity databases through unique personal identifiers. It also proposed a better means of identifying children, as the current system of birth

13 Swahili for "identification".

certificates was prone to duplication of numbers since it was organised around semi-autonomous regional registries. Experts also advised the government to advance from the verification of documents to the authentication of persons, through biometrics (World Bank Group, 2016).

In 2019, an amendment to the RPA was passed to establish the National Integrated Identity Management System (NIIMS), popularly known as *huduma namba* (Statute Law (Miscellaneous Amendments) Act, 2018, 2019). The amendment also expanded data collected during the registration of a person to include biometric data, as well as DNA and GPS coordinates of their home address, although the collection of DNA and GPS coordinates was subsequently nullified by the Kenyan High Court's judgement. The judgment has been appealed (NIIMS judgement para. 1047 (I) and heard but the Court of Appeal had yet to give direction on the matter by the time of writing).

In 2020, the government embarked on a fresh identity enrolment exercise. To enrol, a person was required to bring along all identity documents in their possession. These could include national identity cards or passports for adults, any other functional identity documents such as driving licences, national health insurance cards and national social security cards. During this exercise, the government also enrolled children, using their birth certificates and facial photographs. Copies of the documents and, in some cases, the unique numbers, were recorded. Digital fingerprints of adults and facial photographs of both adults and children were taken (Muraya, 2019).

The exercise and the legal amendment enabling these changes were challenged in a High Court petition in 2020 on the grounds that the legal amendment was enacted without sufficient input from the public. There were also concerns pertaining to the privacy and protection of identity data as well as fears of discrimination against persons who did not have any primary identity documents and who could, therefore, not enrol. This was especially urgent because the government had made it mandatory to have the new digital ID to access government services (NIIMS Case, 2020, para. 537).

Pursuant to the NIIMS judgement, the Executive in 2020 issued two subsidiary legislations known as the Huduma Regulations - the Registration of Persons (NIIMS) Rules, 2020, and the Data Protection (Civil Registration) Regulations, 2020. These regulations establish NIIMS as the primary source of identity data and create a legal basis for the collection of digital data as required under the Data Protection Act. Media reports indicate that the government has printed *huduma* cards for those who enrolled, though many remain uncollected (Kirong', 2021). At the time of writing this report, people who had turned 18 had applied for a national identity card using the processes under the Registration of Persons Act, and the national ID was still valid. Both the *kipande* as well as the *huduma* card were therefore valid.

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The main law governing registration of persons in Kenya is the Registration of Persons Act of 1947. Section 6 of the Act makes it mandatory for every citizen

who reaches the age of 18 years to present themselves for registration before a registration officer.

The enabling framework for digital ID in Kenya is found in an Executive Order, an amendment to the national ID law, two sets of subsidiary legislation, and a judgement from the High Court, as follows:

- In 2018, the President issued an Executive Order directing the development of a central master population database to be the "single source of truth" on all Kenyan citizens and foreign nationals residing in Kenya (Executive Order No.1 of 2018, 2018).
- Later the same year, an amendment to the Registration of Persons Act was inserted into an omnibus Bill and passed in 2019 (Statute Law (Miscellaneous Amendments) Act, 2018, 2019, p. 321). The amendment to this Act created a new system for population management, the National Integrated Identity Management System (NIIMS), which is popularly known as *huduma namba*. The amendment creates a legal basis for the creation of a national population register.
- The question of whether the NIIMS amendment intended to expand the registration of persons from Kenyan citizens to all other residents was amongst the issues canvassed in a case challenging the system (NIIMS case). The case, which was decided in January 2020 by the High Court, considered (among other things) whether the government had a basis for collection of children's data for the NIIMS digital ID project.
- In October 2020, the Executive published two sets of subsidiary laws to give further effect to digital ID. These are the Registration of Persons (NIIMS) Rules and the Data Protection (Civil Registration) Regulations, collectively referred to as Huduma Namba Regulations.

One of the grounds in the petition was the procedure for the amendment. Petitioners contested its rushed passing, the use of a miscellaneous procedure to make a substantive change to the law, and the lack of involvement of one chamber of Parliament in the enactment of the law. The *huduma namba* amendment was passed through a miscellaneous amendment Bill, a procedure typically used for minor legal amendments. Considering that the amendment Bill contained 67 other laws, petitioners argued that the public was denied the opportunity to debate the rationale behind the law. In addition, the law was hurriedly passed without sufficient public input, contrary to the Constitution which provides for public participation in law-making. In addition, the law was only considered at the National Assembly, leaving out the other chamber of Parliament, the Senate. The court, however, validated the procedure used.

Petitioners blamed procedural inefficiencies for gaps in the law such as failure of Parliament to expressly expand the law to apply to all Kenyan citizens and residents, rather than only to adult Kenyan citizens. The Court, while noting that the NIIMS amendment was hurriedly and untidily done, inferred an intent by Parliament to expand the scope of registration of persons to all citizens and residents, including children. As it stands, the amendment to the RPA was validly enacted.

Overall, the judgement ordered for the enactment of an "appropriate and comprehensive regulatory framework" (NIIMS case 2020, para. 1047 (III)) for digital ID prior to the rollout of the programme. In response, the Executive developed and later gazetted two sets of subsidiary legislation that attempt to address the issues raised in the NIIMS judgement.

The Registration of Persons NIIMS Rules make NIIMS the primary source of identification in Kenya (Registration of Persons (NIIMS) Rules, 2020, Rule 10), while the Data Protection (Civil Registration) Regulations create a legitimate basis for processing NIIMS data (Data Protection (Civil Registration) Regulations, 2020 Regulation 4).

By issuing the regulations and appointing a Data Protection Commissioner, the government believes that it has fulfilled the order for an "appropriate and comprehensive regulatory framework" (Tanui, 2020). Arguably, the regulations were made by the Executive and did not go through the rigour and debate expected of a parliamentary legislative process. In addition, their scope was limited to issues covered by their parent Acts (the RPA and the Data Protection Act (DPA)). Hence, *huduma namba* is being implemented without an overhaul of the RPA to establish a more robust system for registration of persons that aligns to the constitutional provisions on citizenship. Issues such as governance of the digital ID system, oversight of the system and its processes and the resolution of complaints are not sufficiently covered.

QUALITY OF LAW

The NIIMS amendment was enacted through an omnibus Bill, the Statute Law (Miscellaneous Amendments) Act, 2018. One of the grounds of the NIIMS case was that the law had such a significant impact on the lives of Kenyans that it should have been a standalone Bill. For example, the amendment, together with pronouncements by government officials, indicated that the new digital ID system would be used for national security purposes. A digital ID would also reportedly be required for access to government and private services (Koech, 2019; NTV Kenya, 2019). This creates uncertainty about access to socio-economic

rights such as education for children and health services for persons without identity documentation. While the court noted that the law was not thoughtfully considered (NIIMS case, para. 813), it declined to declare that there had been a defect in the legislative process. It instead ordered the curing of any issues with the law through "an adequate and comprehensive" framework for digital ID.

Another ground in the NIIMS petition was the discrimination against people who did not possess primary identification documents. The court heard that immigrant communities such as the Nubians, who have been present in Kenya since World War I, still faced difficulties obtaining a national ID. Nubians are a community descended from soldiers enlisted by the British from South Sudan during World War I (ACERWC, 2011). They were thereafter settled in Kenya but have not been officially recognised among the tribes of Kenya, something they blame for the additional procedures they are subjected to when applying for the document. They were subjected to vetting and sometimes security scrutiny to establish their descent. They therefore sought the Court's intervention to protect them from being left out of the new system, particularly since the government was keen on making *huduma namba* a mandatory precondition to access government and private services (ACERWC, 2011). Although the court did not find any discrimination, the potential for discrimination was among the issues that the government was ordered to address in an "adequate and comprehensive" legal framework.

The Huduma Namba Regulations do not address issues of persons without primary identification documents. This is despite there being several reports that call upon the government to address issues of lack of documentation and statelessness. For example, the Sharawe Report (2008) identified the particular issues faced by Muslims, including during application for citizenship documentation. Similar issues have been raised in reports prepared by national human rights institutions (KNCHR, 2007; KNCHR & UNHCR, 2010). The African Commission on the Rights and Welfare of the Child, for example, also recommended that the government address documentation of Nubian children to alleviate problems faced by them later in life as they pursue citizenship documentation. These problems include an inability to participate in life, since the national identity card is required for almost all aspects of life, from movement to employment and access to education. Lack of identity documentation among adults also affects children, since parents cannot register births without the national identity card.

Civil society groups working on issues of citizenship and inclusion expected

the repeal of the RPA and creation of a more inclusive framework to address issues of citizenship documentation. This would include, for example, shifting the burden on citizenship registration from the citizen to the government, addressing historically excluded persons and eliminating statelessness. An ideal situation would be that once a person has been registered, say at birth, the government would provide all other required documentation to the person when needed (KHRC, 2019). However, the amendment to the RPA did not incorporate citizenship guarantees under the Constitution and citizenship laws.

CLARITY AND PRECISION OF THE LAW

The pouring of new wine (digital ID) into old skins (colonial ID) has its problems. First, the language in the old ID law is colonial, with the object of policing the people. For example, it criminalises failure to take out an identity card for a Kenyan adult (RPA, 1947, Section 14 (1) (a)). It also provides significant administrative discretion on the part of the Registrar of Persons and to registration officers through text such as "any other documents may be required" (to ascertain citizenship) (RPA, 1947, Section 8A). Hence, a registration officer can decline to take an application for ID, or refer a person to their rural home to make the application for an identity card there.

Second, and related, the document is tied to citizenship, yet Kenya is a young country where many claims of national citizenship have not been met. People who come from near the border and non-white immigrants such as the Arabs, Makonde, Nubians, Shona and many others have had to constantly advocate for recognition of their communities to facilitate the process of obtaining their citizenship documents (KNCHR, 2007; KHRC, 2020; UNHCR *et al*., 2015).

Third, security issues such as border management and anti-terrorism have created a new basis for vetting of some communities. Following the Security Laws Amendment Act in 2014, more thorough vetting of communities like the Somali and Nubians, who are also Muslims, has taken place. Therefore, even groups like Nubians (who were previously able to obtain identity documents) now face unpredictable procedures in this context. Somalis, who are already recognised as an ethnic group, also face the same administrative unpredictability (Waziri, 2019; Haki na Sheria Initiative, 2020).

2.2 LEGITIMATE AIM

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

The objects of the digital ID programme, NIIMS, are found in the amendment to the primary law on the registration of persons. Section 9A(2) of the Registration of Persons Act lists 10 functions of NIIMS. These can be classified as relating to the creation and maintenance of the population register, the security of the data, updating of the data, and correction of errors in the data.

NIIMS also has functions that give a basis for the centralisation of data. These include, for example: the assignment of unique personal identifiers, presumably to link all identity documents to one person; the harmonisation of government data related to registration of persons; the central printing of identification documents (both primary and functional); the standardisation of identity documentation; and the issuance of a single identification document. The functions of collation and verification of identity data also serve the object of both creating the population register and centralising the data (RPA, 1947, Section 9A (2)).

Although an aim such as issuance of unique personal identifiers could be justifiable, its broad framing creates the risk of government overreach. For example, the desire for unique identifiers for all persons in the population means that children are also included. However, children are a protected group, deserving of special protection. Yet, the provision on unique identifiers or establishment of NIIMS does not envisage any such protections. On the contrary, law enforcement agencies have warned that children found to be in conflict with the law could be marked in security databases, using their unique personal identifiers (Muriuki, 2018). This therefore points to the need for a law that narrows down reasonable grounds under which digital identity data can be accessed.

Another issue arising from the RPA as the digital ID law is the RPA's arbitrary nature. For example, NIIMS greatly expanded government discretion on how people access government services without corresponding checks and balances. The RPA's provisions on NIIMS, together with Huduma Namba Regulations, also lock out persons who are unable to get current ID cards, without any reference to the resolution of identity documentation problems for the vulnerable and marginalised. This is partly why the NIIMS judgement (2020) ordered a comprehensive and adequate legal framework to address issues such as exclusion, access to government services as well as privacy and data protection.

2.3 DEFINING ACTORS AND PURPOSE

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 purposes under the RPA were initially narrow and limited to identification and verification of identity documents (RPA, 1947, Section 2). Registration was also linked to control of movement of Africans. Therefore, the RPA makes it mandatory for people who have reached 18 years to present themselves for registration, or risk criminal sanctions. The identification card must also be produced on demand (RPA, 1947, secs 9 and 10). The 2019 amendments to the RPA extend the purposes of the system. New purposes include verification of persons through biometrics (in addition to validation of identity documents); issuance of unique personal identifiers that effectively track a person's dealings with government from birth to death; centralised issuance of functional identity documents; and standardisation of identity documents (RPA, 1947, sec 9A).

The actors under the RPA were initially limited to citizens who present themselves for registration, the National Registration Bureau (NRB) and law enforcement officers. An authorised public officer can inspect and make extracts from the register of persons (RPA, 1947, Section 5(2)). NIIMS introduces other actors, such as the Principal Secretary, who is "responsible for the administration, coordination and management of the system" (RPA, 1947, Section 9A (3)).

The Huduma Namba Regulations empower public agencies to request access to data held by a civil registry. They also provide for civil registries and other public agencies to link to NIIMS for purposes of the authentication of persons, and transmission, access or retrieval of foundational data required in their duties. The Regulations do not identify the particular agencies that may request data or the criteria to be used in considering such requests (Data Protection (Civil Registration) Regulations, 2020, Rule 18; Data Protection (Civil Registration) Regulations, 2020, Regulation 21).

During the NIIMS case, the government denied any intentions of monetising the NIIMS data and instead stated that the project's primary aim was to create a master population database for more efficient government service delivery. The RPA and the regulations are similarly silent on use of the NIIMS database by private entities, leaving questions regarding their ongoing access to the national identification database.

Besides the RPA, there are other laws under which national identity data is shared. This can happen, for example, through verification of identity documents such as identity cards, car log books, or tax registration cards by private entities. This is provided under various laws such as the Transport Act, which allows a person to apply for a copy of records of motor vehicle ownership or tax laws to support verification of identification records. With the uptake of know-your-customer (KYC) practices in sectors such as banking and insurance, getting a copy of records has been digitised. Employers and people in private transactions, such as the sale of motor vehicles, access the databases to verify tax registration and motor vehicle ownership information. While the practise under these laws is to

provide a copy of records to the public, there is also evidence of public agencies sharing their data with other agencies. For example, the Kenya Revenue Authority (KRA) has related its database with that of the national power provider Kenya Power in order to "catch" people who had multiple power meters. Such people, the KRA presumed, were landlords who needed to pay rental income tax (Okoth, 2019).

In addition, the government maintains a database called the Integrated Population Registration System (IPRS), a collation of identity information from several public agencies. IPRS is managed under the Kenya Citizens and Foreign Nationals Management Service Act (KCFNMA), which collates the management of four identity-related laws.[14] Since 2016, it has been charging for use of the IPRS database. Private entities such as banks, insurance companies and mobile network operators can query the IPRS to verify customer identification documents. In a video interview, the former director of the project based on KCFNMA explains the goals of digital ID as part of Kenya's digital transformation. KCFNMA appears to have the same goals as *huduma namba*, namely the digitalisation of identification information as well as integration of all identity related government services (The Elephant, 2017). However, Huduma Namba Regulations do not link to KCFNMA, leaving in place two systems of identification of persons and documents.

2.4 REDRESS MECHANISMS

Does the law provide for adequate redress mechanisms against actors who use the digital ID and govern its use?

The RPA does not envisage any engagement with citizens, other than for purposes of registration and updating of details. The 2020 Huduma Namba Regulations, however, make provisions for the achievement of the rights of data subjects, flowing from Kenya's Data Protection Act (2019) (DPA). These include the right to be informed of the purpose and uses of the data collected. Regulation 16 creates an obligation for civil registration entities - such as the National Registration Bureau, the Civil Registration Service, the Registrar of Marriages, the Department of Immigration, the Registrar responsible for Children Affairs, the Department of Refugee Affairs and the Principal Secretary responsible for the NIIMS database - to notify users in simple language about issues in Section 29 of the DPA. These include notifications about the fact and purpose of data processing as well as the rights of the data subject and consequences for the data subject should they fail

14 These are the Citizen and Immigration Act, 2011 (Chapter 3), Births and Deaths Registration Act (Chapter 149), Registration of Persons Act (Chapter 107) and Refugees Act, 2006.

to provide all of the requested data. Other requirements under Section 29 are notifications to the data subject of all actors (such as the controller, processor, any third parties) involved in data processing, as well as technical and organisational measures for the integrity of the data.

However, at the time of writing this report, civil registries had not yet implemented this regulation. Citizens and residents whose data is held by the various registries have not been informed of the purposes and uses of their data. The only communication people who enrolled for *huduma namba* during the 2020 mass enrolment exercise have received is SMSes notifying them that their *huduma* cards were ready for collection or informing them about the collection point for their cards (Kejitan, 2021).

ACCESS AND CORRECTION

The RPA contains limited instances where people can engage with registration officers. These are upon initial registration, for the replacement of identity cards, and after a change of names, for example upon marriage (Registration of Persons Rules, 1948 Rule 9(2)).

Civil registration entities rely on provisions of the parent law, e.g., the Birth and Death Registration Act, for the correction of details such as names. These registries have been digitalising their records in the past decade, making them subject to the data protection law. From a data rights perspective, data subjects should have the right to know what data about them is held by the entity, to object to the processing of their data, and to request the amendment or deletion of incorrect or misleading data about them. The Data Protection (Civil Registries) Regulations require civil registration entities to give access to data subjects and also provide for mechanisms for rectification of data.

At the time of writing this report, no civil registration entity had created a fully functional mechanism for access and rectification as required under the DPA.

DUE PROCESS

The RPA was amended in 2018 to provide for the cancellation of registration and the revocation of identity cards. The grounds for cancellation and revocation are listed as the misrepresentation and concealment of material facts, fraud, forgery and multiple registration (RPA, 1947, Section 18A). The amendment requires the Director of National Registration to give a 14-day notice to show cause to the person facing deregistration. There is also a 15-day period after a deregistration and revocation decision to allow for appeal to any court with jurisdiction over the Act (RPA, 1947, Section 18A (3)).

The Huduma Namba Regulations require each civil registration entity to

establish an internal complaints procedure (Data Protection (Civil Registration) Regulations, 2020 Regulation 23). This means that a data subject can lodge a complaint about data processing with the civil registration entity. A search on the portals of civil registration entities as well as the e-government portal shows that the civil registration entities have not implemented this measure. The registries are depending on provisions for amendment of information that exist in their parent laws. They are yet to formulate procedures on issues that are not provided for in the parent law, for example the right to know what data an entity holds about a person. In practice, this means that people with identification documentation problems either have to physically visit the offices of the civil registration entity or seek representation from civil society advocacy groups. Some civil society groups, for example the Haki na Sheria Initiative and the Nubian Rights Forum, have paralegal programmes to assist applicants for identity documentation.

2.5 ACCOUNTABILITY

The RPA was enacted primarily to enforce the registration of persons. It does not, for example, create a body corporate to oversee the registration of persons. It does, however, create a layer of bureaucracy in the form of a hierarchy of registration and fingerprint officers under the NRB. These officers are appointed by the Cabinet Secretary (RPA, 1947, Section. 4). In areas without adequate registration officers, people have to typically petition the cabinet secretary to appoint more officers (KHRC, 2019).

NRB officers have police and quasi-judicial powers and can arrest people suspected of contravening the RPA ((RPA, 1947, Section 17A) without a warrant. The Director of the NRB can revoke fraudulent or fake national identity cards (RPA, 1947, Section 18A). Despite these broad powers, there is no specific accountability mechanism such as periodic reporting to a parliamentary committee under the Act.

A 2014 amendment to the law gave the Director of the NRB the power to establish committees to assist with identification of persons. These committees are popularly known as vetting committees and are prevalent in border areas as well as in areas where minority communities such as Nubians live. According to the law, their role is to “assist in the authentication of information furnished by a parent or guardian” (RPA, 1947, Section 8A). The committees typically consist of security agents, local national government officials such as chiefs or sub-chiefs, and elders from the community. They usually sit a few times every month to consider applications for national identification cards (NIIMS case para. 99).

For applicants undergoing vetting, the process involves presenting themselves for an interview during the vetting committee sitting. They then have to follow up, typically by checking during subsequent vetting sittings, to see if their application

has been approved and forwarded to the NRB. Where no information is forthcoming, some start a fresh application, while others visit higher government offices. The lack of information on the process and the lack of accountability on the part of vetting committees are gaps that need to be addressed.

The experience of vetting demonstrates how administrative procedures can create barriers to the right to have a legal identity. Although the committees are not required to report to the public, members of Parliament have on various occasions questioned some of the practices of the NRB. They have often succeeded in putting pressure on the bureau to issue identity cards, particularly around general elections, when there are many young people seeking the national identity card in order to be registered as voters. For example, prior to the 2017 General Elections, amendments to the RPA included the setting of timelines for the production of identity cards; cards are now supposed to be issued within 30 days of applying. In addition, the Cabinet Secretary for Interior was empowered to provide guidelines on vetting. The thinking was that guidelines would make the vetting process less discretionary by giving applicants information on vetting requirements for new and replacement cards (RPA, 1947, Section 16 (ba)). However, all amendments to the RPA have failed to overhaul the system and create a new system with a robust governance mechanism.

2.6 MISSION CREEP

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

The digital ID system and its precursor national ID are also part of the national security system. They are issued by the NRB, which is a department of the Ministry of Interior and Co-ordination of National Government. Law enforcement officers get access to national identity card data through processes such as acquiring a police clearance certificate - a document required for most public job applications (Ong'era & Musili, 2019).

To obtain a police clearance certificate, a person presents themselves to have their fingerprints taken by the police. The fingerprints are then run against a database of criminal records maintained by the police. The criminal database is provided for under the National Police Service Act (2011). The law provides that information about criminal investigations should be destroyed if a person is not charged, or on discharge or acquittal. This provision, coupled with the practice of fingerprinting, gives law enforcement officers access to the national identification database for purposes of matching fingerprints. However, there are no regulations on data sharing between law enforcement officers and the NRB, leaving room for unfettered use of identification data by law enforcement officers, without safeguards.

For example, in the past few years, the Directorate of Criminal Investigation (DCI) has tweeted warnings to students about the consequences of delinquency, in a manner to suggest that they have access to identification data. Following a spate of school fires, the DCI warned that fingerprints and other identity information of students suspected of such behaviour would be captured in security databases and shared with prospective employers (Muchunguh, 2021; Muriuki, 2018). It is not clear if this was a threat meant to deter students from delinquent behaviour or an indication that law enforcement officers have access to education system databases.

Mission creep can also occur where the government obtains data from other sources. An interesting example is the case of double registration affecting Somali people in three counties in Kenya. These people were taken to refugee camps, many of them as children, from the late 1990s. Fingerprints were taken as part of UNHCR administrative procedures in issuing food and providing medical and relocation support to the refugees. Later, as they attained the age of majority and attempted to apply for national ID cards, they found out that UNHCR had handed over the refugee registration database to the government of Kenya. Their application for the Kenyan national identification card was therefore rejected, as they were marked as refugees. Through civil society efforts, they advocated for deregistration from the UNHCR database. From late 2019, the government undertook to address their plight. They were requested to provide documents supporting their citizenship claims, for example school certificates and letters from local leaders. Their applications are reportedly being vetted. However, many of their cases are yet to be resolved and they therefore do not have national identity cards (Haki na Sheria Initiative, 2020).

The case illustrates how the sharing of data among public agencies or even humanitarian agencies can have dire consequences on real people and highlights the dangers of mission creep. For example, without an identity card, one cannot freely travel outside the county, as the document must be produced at roadblocks. One also cannot access higher education, or register a child's birth, as all these processes require an identity card. People without identity cards cannot directly participate in the mobile telephony economy, as Kenya has mandatory SIM card registration laws, and neither can they operate a mobile money account in their own name.

The acquisition of the UNHCR database (mentioned above) is viewed by the government as a security measure aimed at curbing the illegal registration of identity documents. However, the reasons that led people to register as refugees - famine, the search for better opportunities, and a lack of government services in the area - are not considered. Government agencies are arguably still not doing enough to provide registration and other attendant services such as maternity centres to marginalised areas. The implicit or explicit security functions of

identity documentation seem to take precedence.

The NIIMS judgement called for the development of data sharing codes among government agencies, a measure that would provide some safeguard against mission creep. However, the Huduma Namba Regulations are broad enough to allow access of data by law enforcement (Data Protection (Civil Registration) Regulations, 2020 Rule 18). The Regulations only require that such a request be written and specific. However, they do not limit the nature of data that may be accessed, leaving that decision to administrative discretion and oversight (Data Protection (Civil Registration) Regulations, 2020 Regulation 21). In view of the broadness of issues of national security, independent oversight is required to avoid mission creep if law enforcement and other national security organs have access to data. This is currently lacking under the RPA and Huduma Namba Regulations.

RIGHTS-BASED TESTS

3.1 NECESSITY AND PROPORTIONALITY

Are the privacy violations arising from the use of digital ID necessary and proportionate to achieve the legitimate

aim?

One of the issues of contention in the NIIMS case was the proportionality of some of the data points , for example DNA in digital form, and GPS coordinates of home addresses. Petitioners also argued that it was not necessary to collect a lot of the data currently required about children, since they do not access any services on their own because they do not have legal capacity. The court found that the reasons put forward by the government for collecting DNA and GPS data were not sufficient to warrant the invasion of privacy. The provision on collection of DNA and GPS data was therefore nullified (NIIMS Judgement, 2020, para 1047(I)).

The RPA has been mandatory for adult citizens since independence. It must be produced on demand, and failure to register for the document attracts criminal sanctions (RPA, 1947, Sections. 10 and 14). It has acquired usage as an identity document for various functions from acquisition of other documents, employment, voting and access to higher education. This effectively means that personal data contained in various government and private databases can easily be related, since the national ID details are used as the unique identifier when creating the information in those databases (KNCHR, 2007).

Normalisation of the use of the national identification card number in almost every transaction in Kenya makes identity key for access to fundamental rights. At the same time, it gives impetus for higher standards of protection of personal data, since the national identification number can provide granular information about a person,

The RPA does not envisage digital sharing and therefore has only broad provisions on collection, collation and integration of data to create a single source of personal information for all citizens, residents and anyone present in Kenya (RPA, 1947, Section9A (2)). This is a broad provision that requires elaboration on the reasonable grounds on which data can be used, as well as a description of actors that can access this data.

It is worth noting that while these are Huduma Namba Regulations, which were meant to provide further detail to the RPA, they do not address issues such as the use of data already collected. For example, the collection of data on ethnicity has been contentious, yet data continues to be collected. Even if there were privacy safeguards, it leaves questions about why the government would need such granular data on the identity of people, and whether there are less invasive means of achieving the same ends.

3.2 DATA MINIMISATION

Are there clear limitations on what data may be collected, how it may be processed and how long it is retained for,

during the use of digital ID?

The RPA specifies biographic and demographic data to be collected when applying for an identity card as: name, date of birth, age, sex, occupation, county of birth or residence, place of residence, biometric data and date of registration. Biometric data includes fingerprints, hand geometry, earlobe geometry, retina and iris patterns, and voice waves (RPA, 1947, Section 3). The 2018 RPA amendment had attempted to add the collection of DNA and GPS data. However, the court annulled these two data points, noting that their collection was invasive, yet their collection had not been specified in law (NIIMS Judgement, 2020, para. 1047 (I) and (II)).

Information about one's parents is also required. The provision includes "any other information that may be required" and this has in the past been used to demand further proof of descent (RPA, 1947, Section 8(1)). The form used to collect information during enrolment into the NIIMS requires biographic and demographic data such as family relations, education details, employment details and agricultural activities. In addition, data on functional identities, such as the applicant's national social security number and national health insurance number, are requested.

During the NIIMS hearing, government officials explained that data such as education, employment and agricultural activities had been requested by other ministries (NIIMS Judgement, 2020, para. 352). However, and from a data sharing perspective, there are no safeguards on how that data was transmitted to the requesting ministries and whether a copy of that information would remain in NIIMS.

3.3 ACCESS CONTROLS

Under the old RPA regime, access to the register was limited to public servants with authorisation from the Cabinet Secretary. The Data Protection (Civil Registration) Regulations require each civil registry to have access permission management, documentation on security access as well as records of security incidents. It is noted, however, that the Regulations leave it to each registry to develop its own protocols and do not elaborate principles on access controls (Data Protection (Civil Registration) Regulations, 2020 Regulation 21) .

3.4 MANDATORY USE

As stated earlier, Kenya has a long history of mandatory use of the national identity card. Despite this, the document is not available to every person, with research showing that people from border communities and ethnic minorities have reduced access to citizenship documentation. The lack of a national identification card in Kenya excludes people from many services, including

anything from movement outside their home area to opening a bank account or registering a mobile number. It is expected that the mandatory use of *huduma namba* for identification and authentication of people will exclude not only those individuals without primary identification documents, but also people from areas where government services are not easily accessible. This includes areas that are underserved in terms of electricity and internet connectivity.

Analogies can be drawn from the 2017 elections, when voter identification could not be done online due to disparate internet availability in the country. When it came to using technology for transmitting election results, there were areas where results transmission was delayed as election officials had to travel to the nearest area with internet connectivity (KICTANet, 2017).

The country is now moving towards the registration of children. This has already begun through a mandatory requirement to register every child on the national education management information system (NEMIS). The implementation of the directive has faced challenges such as a lack of birth certificates, which deterred some children from attending school; a high demand for birth certificates, which created opportunities for corruption; as well as difficulties in registering birth certificates on NEMIS due to similarities in birth certificate numbers.

The requirement for a birth certificate was temporarily halted to reduce disruption to learning. However, in many registration centres, parents are still pursuing birth certificates for their children to ensure that they do not miss out on education and national examinations. In the case of women without national identity cards, which are required for birth registration, people seek various means to get the registration, including getting their children registered using other women's identity cards (NRC, 2017).

NIIMS is set to become the primary means of identification for public and private services. The Registration of Persons (NIIMS) Rule 10 states:

> *Any Government agency requiring personal particulars of an individual shall, at the first instance, rely on the NIIMS database to authenticate the foundational data of an enrolled resident individual.*

It is not clear if, without it being a legal requirement, public agencies would consider other forms of identification. Most agencies tend to be short-staffed, placing a burden on people seeking services to comply as closely as possible with their requirements.

RISK-BASED TESTS

4.1 RISK ASSESSMENT

Are decisions regarding the legitimacy of uses, benefits

of using digital ID, and their impact on individual rights informed by risk assessment?

A 2016 country assessment by the World Bank noted the lack of a data protection law in Kenya and recommended that one be enacted. Unsurprisingly, one of the issues raised in the NIIMS case was the potential for repurposing NIIMS data, in the absence of a privacy and data protection law. For example, in view of the risk posed by the centralisation of data, the petitioners sought to know the architecture of the project, and the mechanisms applied to implement principles such as privacy by design.

Although the Data Protection Act was enacted in 2019, processing of data for national security or public interest is exempted from certain provisions of the Act, for example specification of purpose, acquisition of consent from the data subject and perpetual retention (DPA, 2019, Section 51). In the NIIMS judgement (2020), the Court noted that there was a need to implement the law to mitigate against some of the threats raised by petitioners. The court called for development of regulations to give effect to the DPA on issues such as the protection of data in general and the protection of children's data specifically. The court also noted the need for data sharing codes among public agencies and risk mitigation for groups at risk of exclusion from the digital ID programme.

During the NIIMS case (2020), the government confirmed that it did not conduct a risk assessment on privacy as well as other rights including freedom from discrimination, the rights of children and women, or economic and social rights. The Huduma Namba Regulations give guidance on how to carry out a data protection impact assessment by civil registration entities. The regulations do not, however, make it mandatory to carry out this assessment (Data Protection (Civil Registration) Regulations, 2020 Regulation 19).

Yet, many remain hopeful that, with the appointment of the Data Protection Commissioner, civil registries will be asked to carry out data protection impact assessments. This is particularly urgent in light of upcoming general elections in 2022. With previous experiences of poor standards of personal data protection on voter rolls, there is likely to be political pressure to mitigate risks arising from digital identity data. During the 2017 elections, for example, there were instances where personal data from voter rolls such as national identity card number and phone number were exposed for automated data mining (Kenya ICT Action Network, 2017).

4.2 DIFFERENTIATED APPROACHES TO RISK

Do the laws and regulations envisage a differentiated approach to governing uses of digital ID, based on the risks it entails?

Although the court in the NIIMS judgment (2020) declined to find that there was discrimination under NIIMS, it underlined the risk of exclusion for groups that have historically had challenges in accessing identification documentation. Measures to mitigate such risk were among the issues that were expected to be addressed in the framework that the court ordered prior to the implementation of NIIMS. However, the Huduma Namba Regulations, which were developed pursuant to the judgment, do not address the issue of risk. The Regulations limit themselves to operationalising NIIMS through the enrolment of people.

The NIIMS case (2020) also discussed the risks posed to children. The judgment highlighted the need to act in the best interest of children in view of their limited capacity and also to ensure that their evolving capacity was taken into consideration when handling their data. While it was expected that the framework pursuant to the judgement would encompass special collection of children's data and also transition from childhood to adulthood, the Regulations are limited to the definition of a child and the requirement for parental or guardian's consent when processing children's data (Data Protection (Civil Registration) Regulations, 2020 Regulation 15).

The lack of an independent governance structure, such as a dedicated service or body for identity administration, has been raised in various reports and meetings of civil society (KHRC, 2019). In 2019, the government revived the taskforce to develop vetting criteria and modalities for registration of stateless persons (Matinag'i, 2019). The Shona community, who descended from southern Africa, will be among the first to benefit from citizenship by registration under this commitment (KHRC, 2020). However, for communities claiming citizenship by descent, which is irrevocable, the risk of exclusion from government services due to a lack of identification documentation still remains.

Previously, groups have resisted biometric registration for fear of criminalisation. In one case, a consortium of NGOs working on HIV issues sued the Cabinet Secretary for Health over a plan to biometrically register HIV patients getting government treatment. The court agreed that such registration posed grave privacy concerns and halted the project. It also ordered the coding of any data that may have been collected to protect the privacy of patients (KELIN & Kenya Key Populations Consortium, 2018). Attempts to register government workers have similarly been met with resistance, with the workers seeking assurance that their data will not be used for other purposes (Alushula, 2021).

4.3 PROPORTIONALITY

Does the law on digital ID envisage governance, which is proportional to the likelihood and severity of the possible risks of its use?

NIIMS envisages the correction of inaccurate information by the data subject (RPA,1947, Section 9A(2). However, this provision has not been actualised, owing to the logistical challenges that already exist in registration of persons, let alone correction of inaccurate data. For example, birth registration is still a challenge in rural and underserved areas (National Assembly, 2020). While one can make a written application for correction of inaccurate information under the Births and Deaths Registration Act, it was expected that digital systems would provide more convenient means for correction of inaccurate information.

The government has stated on numerous occasions that it is cleaning data in its registries so that NIIMS can be an authoritative primary source of identity information. For example, in the case of double-registered people, their other documents (such as example school-leaving certificates and parents' identity cards), are being verified so that their fingerprints can be removed from the UNHCR refugee database (Astariko, 2020).

AUTHENTICATION ERRORS

Public agencies are yet to put NIIMS into use, particularly for purposes of authentication. This is partly because *huduma namba* is not yet fully operational, as not every eligible Kenyan has been issued with the card. In addition, the current legal framework still supports using the national identification card. However, experience from the previous two elections, where voter identification failed on the day of the general election, points to the need for thorough testing and a pilot period before full rollover to the new system (especially before the 2022 election).

The law does not specifically provide for dealing with authentication errors. The Data Protection (Civil Registries) Regulations contain provisions on automated decision-making that are applicable to authentication. Regulation 22 (d) requires an entity that uses automated decision-making to "ensure the prevention of errors, bias and discrimination". Such an entity is also required to minimise errors by putting in place appropriate mechanisms to prevent them. There are, however, no guidelines on how to mitigate against authentication errors, for example through the use of alternative methods of authentication, as was the experience with elections (USAID, 2014). Following experiences with authentication errors in the 2013 election, election procedures were amended to allow for persons who could not easily be authenticated to be physically authenticated (Elections Act, Section 44A).

IDENTITY THEFT

The use of another person's identity card, as well as the unauthorised production of identity cards, is criminalised under Section 14 of the RPA. Impersonation and identity theft are also offences under Section 29 of the Computer Misuse and Cybercrimes Act.

In the past, weaknesses within the NRB resulted in the production of fake identification cards (KNCHR, 2007). Some of these cards had similar numbers to existing authentic ones. Consequently, the law was amended to empower the Director of the NRB to revoke fraudulently acquired identity cards (RPA, 1947, Section 18A). According to the government, identity fraud is still a problem, hence the need for physical authentication of people in addition to their documents being authenticated (World Bank, 2016).

MISSION CREEP

The Data Protection Act contains principles to protect against the repurposing of personal data, such as requirements for fairness, transparent processing, data minimisation and data retention. However, the peculiar nature of government service provision, coupled with the framing of national identity as a national security function, makes it challenging to monitor government data processing. For example, access to any government service requires the national identity card for identification. Many functional identities, such as the national social security card, national health insurance and driving licences, are linked to the national identity number. This means that any government agency can easily relate their database with another agency. The phenomenon has already been witnessed in the case of the revenue authority relating to, or seeking to relate to, databases such as the Higher Education Loans Board (HELB), Kenya Power and mobile money operators, for purposes of estimating taxes and catching tax evaders (Business Daily, 2017; Okoth, 2019).

Data is also viewed as a tool for more efficient security by Kenya's security agencies. The government has been reorganising and centralising security agencies' functions such as communication and surveillance (Kenyatta, 2020). Coupled with other legal updates, such as investigation procedures under the Computer Misuse and Cybercrimes Act (CMCA), there is a risk of government overreach in national security processes. For example, the CMCA provides for real time collection of traffic data as well as interception of the substance of communication. Considering that communication is linked to personal identity through mandatory SIM card registration; security officers can therefore infringe the privacy of communications. While the CMCA requires a court order for interception, privacy could be enhanced through oversight, transparency and accountability. This could include independent oversight of data access by security and other agencies, as well as notification to subjects of surveillance and periodic reporting to the public and Parliament.

INDISCRIMINATE DATA SHARING

The Huduma Namba Regulations envisage sharing of data among civil registries

as well as other public agencies requiring the use of NIIMS data. Standardisation of data and interoperability of databases are also objects of digital transformation, as stated in policy documents such as the Integrated Population Registry Strategy Paper (2006) and Government Enterprise Architecture (2016). However, neither these documents nor the RPA provide for checks and balances on data sharing. As stated earlier, public agencies can share data, but there are no data sharing codes governing the process of sharing. In addition, there are no specific oversight mechanisms for governance of digital ID data. The Office of the Data Protection Commissioner (ODPC), which may provide some oversight on data protection, is housed under the Ministry of ICT, raising questions on whether the ODPC is really independent. As such, there is a need for more robust checks and balances.

CONCLUSION

The patching of an old colonial law with a new digital ID law leaves gaps, and makes it difficult to achieve a “comprehensive and adequate framework”, as ordered by the NIIMS judgement. This is because the law was created in a

different constitutional dispensation, where human rights were not explicitly recognised. Questions in the CIS Evaluation Framework highlights several gaps in the current law, including:

- the problematic use of Executive tools, such as directives and subsidiary legislation, to make laws that greatly impact on people's lives. This calls for a new framework to be debated in Parliament, with more meaningful public participation and inclusion of social interests. The law should address those at risk of exclusion by ensuring that they are prioritised in any digital ID law. It should also avoid the mandatory linking of ID with government services, to protect people without ID and people who live in areas without adequate access to digital technology from missing out on social services.
- the lack of legal clarity and precision, which is exacerbated by patching of the national ID law with a legislative provision for digital ID. Existing provisions, such as access to the register by law enforcement, have a great impact in the digital realm because the officers can access more data more readily. Hence, there is the need to restrict law enforcement officers' access to data collected for other purposes.
- the favouring of the government by current laws. For example, linking the digital ID to government services eases data collection. The law could be more centred on the data subject, by providing the person access to their data, as well as their rights - from correction of their data to lodging complaints. There is also need for a governance mechanism to make digital ID authorities accountable to the people and Parliament.

RECOMMENDATIONS

For civil society:

- Advocacy around digital ID issues in Kenya has brought together civil society organisations from different areas. A lesson that has been learnt is that digital ID is a disruptive force touching on many issues, from identity and inclusion to rule of law and governance. There is a need for civil society organisations working on various areas such as social justice and digital rights to join forces. This would allow them to advocate for digital ID frameworks that are not only inclusive, but also protect citizens from technology related harm across a broad range of concerns.
- Digital ID policies for countries such as Kenya are driven by external forces such as development partners. However, their effects are felt by people who are either denied access to government services or experience these services differently. Civil society organisations have the task of bringing to the fore the effects of digital ID policies so as to influence better digital policy making.

For policymakers:

- Digital ID is a complex issue that requires wide consultation and learning. Policy makers should not rush digital transformation. They instead should publish their digital ID plans and consider all input from other stakeholders, particularly those most likely to be affected by digital ID.
- In view of the various levels of technology access in Kenya, policymakers should phase the introduction of digital ID. Digital ID policies and laws should also provide for instances where it is impossible for digital ID to work, for example where there is lack of electricity or internet connectivity.

For technologists:

- Digital ID is not purely a technology problem. Any new technology developed and deployed should be sensitive to the nuances of the country and the situation to which it is to be applied.
- Technologists should also prioritise and advise governments on technology choices that enhance human rights and improve opportunities for a better life, as opposed to stifling it. For example, there has not been as much discussion on decentralised digital ID, whose architecture aligns more with goals such as devolution and decentralisation of power under Kenya's Constitution.

For further research:

Research on digital ID monitoring and evaluation frameworks for different countries and use cases would add to a better understanding of how Kenya can best implement a national digital ID system.

For donor agencies:

Donor agencies should invest in and understand alternative and localised conceptions of digital ID. For example, many donors support centralised digital ID, which creates many risks for human and people's rights.

REFERENCES

ACERWC (2011) *Institute for Human Rights and Development in Africa (IHRDA) and Open Society Justice Initiative (on behalf of Children of Nubian Descent in Kenya) v. the Government of Kenya*.

Aleshia, P. (2021, January 11). SRC taps IT to unearth civil servants secret perks.

Business Daily. *https://www.businessdailyafrica.com/bd/economy/src-taps-it-civil-servants-secret-perks-3253048*

Astariko, S., 2019. Relief as state pardons Kenyans registered as refugees. *The Star*. *https://www.the-star.co.ke/counties/north-eastern/2019-11-08-relief-as-state-pardons-kenyans-registered-as-refugees/*

Atellah, J. (2020, June 14). Toa Kitambulisho! Evolution of Registration of Persons in Kenya. *The Elephant*. *https://www.theelephant.info/data-stories/2019/06/14/toa-kitambulisho-evolution-of-registration-of-persons-in-kenya/*

Balaton-Chrimes, S. (2021). Who are Kenya's 42(+) tribes? The census and the political utility of magical uncertainty. Journal of Eastern African Studies, 15(1), 43–62. *https://doi.org/10.1080/17531055.2020.1863642*

Breckenridge, K. (2019). The failure of the 'single source of truth' about Kenyans: The NDRS, collateral mysteries and the Safaricom monopoly. *Journal of African Studies*, 78(1), 91–111. *https://doi.org/10.1080/00020184.2018.1540515*

Business Daily, 2020. Safaricom rejects KRA bid for free access to taxpayers M-Pesa accounts. *Business Daily*. *https://www.businessdailyafrica.com/bd/economy/safaricom-rejects-kra-bid-for-free-access-to-taxpayers-m-pesa-accounts-2118628*

Nubian Rights Forum and 2 others v. Attorney-General and 6 others; Child Welfare Society and 8 others (Interested Parties), EKLR (High Court of Kenya, Nairobi 2020).

Haki na Sheria Initiative. (2020, December 17). The Plight of #DoubleRegistered Victims in Kenya. *https://www.youtube.com/watch?v=mJQhXGTEipM*

Kejitan, V., 2021. Expect an SMS if you registered for Huduma Namba — Ministry of Interior. *The Standard*. *https://www.standardmedia.co.ke/kenya/article/2001400744/expect-an-sms-if-you-registered-for-huduma-namba-ministry-of-interior*

KELIN & Kenya Key Populations Consortium. (2018). 'Everyone Said No', Biometrics, HIV and Human Rights – A Kenya Case Study [NGO Policy Paper]. KELIN. *https://www.kelinkenya.org/everyonesaidno/*

Kenya Gazette Notice No. 7881 of 23 August 2019. *http://citizenshiprightsafrica.org/wpcontent/uploads/2019/08/Kenya-Taskforce-Identification-Stateless-Persons_Gazette.Vol_.CXXINo.110_23Aug2019.pdf*

Kenya ICT Action Network. (2017). Preliminary Observations on Technology Deployment in Kenya's General Election 2017 [NGO Policy Paper]. *https://lists.*

kictanet.or.ke/pipermail/kictanet/attachments/20170811/356bef8e/attachment.pdf

Khawaja, N. (2018, June 8). Kenya's Identity Crisis. JIA SIPA. *https://jia.sipa.columbia.edu/online-articles/kenyas-identity-crisis*

KHRC. (2019). Digital identification document (ID) and citizenship consultative meeting [Workshop report]. KHRC. *https://www.khrc.or.ke/publications/198-report-of-digital-identification-citizenship-workshop-naivasha/file.html*

KHRC. (2020). African missionaries in identity limbo: The Shona of Kenya. Kenya Human Rights Commission. *https://www.khrc.or.ke/publications/221-african-missionaries-in-identity-limbo-the-shona-of-kenya/file.html*

Kirong', E. (2021, April 28). Huduma cards in Nairobi lie uncollected. *The Standard*. *https://www.standardmedia.co.ke/nairobi/article/2001411128/huduma-cards-in-nairobi-lie-uncollected*

KNCHR. (2007). An Identity Crisis? A Study on the Issuance of National Identity Cards In Kenya [Government Human Rights Report]. Kenya National Commission on Human Rights (KNCHR). *http://www.knchr.org/Portals/0/EcosocReports/KNCHR%20Final%20IDs%20Report.pdf*

KNCHR, & UNHCR. (2010). Out of the Shadows: Towards Ensuring the Rights of Stateless Persons and Persons at Risk of Statelessness in Kenya (p. 70) [Government Report]. KNCHR and UNHCR. *https://www.unhcr.org/4e8338d49.pdf*

Koech, G. (2019, September 28). Criminals to be traced and profiled through DNA, says Matiang'i. *The Star*. *https://www.the-star.co.ke/news/2019-09-28-criminals-to-be-traced-and-profiled-through-dna-says-matiangi/*

Mamdani, M. (2001). Beyond Settler and Native as Political Identities: Overcoming the Political Legacy of Colonialism. *Comparative Studies in Society and History*, 43(4), 651–664.

Muchunguh, D. (2021, January 26). DCI to keep records of students involved in criminal conduct. *Daily Nation*. *https://nation.africa/kenya/news/-dci-keep-record-juvenile-crimes-3268792?view=htmlamp*

Muraya, J. (2019, May 17). Fear drives Kenyans, foreigners to register for Huduma Namba 24 hrs to deadline. *Capital News*. *https://www.capitalfm.co.ke/news/2019/05/fear-drives-kenyans-foreigners-to-register-for-huduma-namba-24-hrs-to-deadline/*

Muriuki, B. (2018, July 8). Warning to all students as DCI announces tough

disciplinary measure. *Citizentv.Co.Ke*. *https://citizentv.co.ke/news/warning-to-all-students-as-dci-announces-tough-disciplinary-measure-206224/*

Nalule, C. (2020). Report on citizenship law: Kenya [Technical Report]. European University Institute. *https://cadmus.eui.eu//handle/1814/66749*

National Cohesion and Integration Commission. (2016). Ethnic and Diversity Audit of Commissions (p. 65) [Government Report]. NCIC. *https://www.cohesion.or.ke/images/docs/Ethnic_and_Diversity_Audit_of_Commissions_2016.pdf*

Ng'weno, B., Aloo, L.O., 2019. Irony of Citizenship: Descent, National Belonging, and Constitutions in the Postcolonial African State. *Law & Society Review* 53, 141–172. *https://doi.org/10.1111/lasr.12395*

NTV Kenya. (2019). Huduma Namba to help in tracking down traffic offenders—CS Matiangi. *https://www.youtube.com/watch?v=14aSrkh81Sk*

Norwegian Refugee Council, 2017. Recognising Nairobi's Refugees The Challenges and Significance of Documentation Proving Identity and Status (NGO Report). NRC, Nairobi.

Okoth, E. (2019, May 30). KRA taps Kenya Power meters to catch landlords. *Business Daily*. *https://www.businessdailyafrica.com/bd/news/kra-taps-kenya-power-meters-to-catch-landlords-2252108*

Ong'era, A., & Musili, B. M. (2019). Public Sector Reforms in Kenya: Challenges and Opportunities (Working Paper Working Paper No. 29 of 2019). The Kenya Institute for Public Policy Research and Analysis (KIPPRA). *http://repository.kippra.or.ke/handle/123456789/2105*

Tanui, C. (2020, September 16). Huduma Namba e-cards production to begin in December: PS Kibicho. *Capital News*. *https://www.capitalfm.co.ke/news/2020/09/huduma-namba-e-cards-production-to-begin-in-december-ps-kibicho/*

USAID. (2014). USAID support for Kenya'S 2013 Elections: Rapid Assessment Review (p. 32). Republic of Kenya, 2010. Constitution of Kenya.

Executive Order No.1 of 2018—Reorganisation of the Government of the Republic of Kenya, No 1 of 2018 (2018). *https://www.theelephant.info/documents/executive-order-no-1-of-2018-reorganisation-of-the-government-of-the-republic-of-kenya*

Registration of Persons Act, Pub. L. No. Cap 107, Cap 107 (1947).

Kenya Citizens and Foreign Nationals Management Service (Charges for use of Information from the Register) Regulations, Legal Notice No 69 of 2016 (2016).

Data Protection Act, (2019).

Statute Law (Miscellaneous Amendments) Act, 2018, Kenya Gazette Supplement No. 161 Act No 18 of 2018 315 (2019). *http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2018/StatuteLawMiscellaneousAmendmentsBill2018.pdf*

Data Protection (Civil Registration) Regulations, Kenya Gazette Supplement No 176, Legal Notice No 196 (2020).

Registration of Persons (National Integrated Identity Management System) Rules, Legal Notice No 195 Kenya Gazette Supplement No 176, Legal Notice No 195 (2020).

Truth, Justice, and Reconciliation Commission, 2008. Commissions of Inquiry - Report on Concerns of Muslim Community (Sharawe Report) (Government Report). *https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1002&context=tjrc-gov*

UNHCR, Haki Centre, & OSIEA. (2015). Integrated, But Undocumented: A study into the nationality status of the Makonde community in Kenya [UN report]. UNHCR.

United Nations. (1969). Methodology and evaluation of population registers and similar systems (Vol. 15). Publishing Service, United Nations. *https://unstats.un.org/unsd/publication/SeriesF/Seriesf_15e.pdf*

Waziri, K. (2019, July 5). The Ones Who Are, But Don't Exist: Being Nubian, and Kenyan. *The Elephant*.

Weitzberg, K. (2020). Biometrics, Race Making, and White Exceptionalism: The Controversy Over Universal Fingerprinting in Kenya. The Journal of African History, 61(1), 23–43. *https://doi.org/10.1017/S002185372000002X*

World Bank Group. (2016). Identification System Analysis: Kenya Country Report. The World Bank Group.

ANNEX 1

OVERVIEW OF EVALUATION FRAMEWORK

In 2019, the Centre for Internet and Society (CIS) published "Governing ID: Principles for Evaluation" ("Evaluation Framework"), which set out a framework for the evaluation of digital identity. The Evaluation Framework should be read alongside CIS' glossary of 'Core Concepts and Processes' that explains different principles such as identification, authentication, foundational and functional identity systems, that are present in any Digital ID system. Early draft frameworks were published in the lead up to RightCon 2019 held in Tunisia and were discussed at an event organized by Omidyar Network titled "Holding ID Issuers Accountable, What Works?"

The impetus for this document came from Clause 16.9 of the UN Sustainable Development goal, "By 2030, provide legal identity for all, including birth registration". Thus, countries across the world have begun implementing new, foundational, digital identification systems ("Digital ID"), or begun to modernize their existing ID programs.

The history of digital ID programmes in countries such as India, Kenya, Estonia, Jamaica, and the U.K. demonstrated the different concerns associated with privacy, surveillance, exclusion, and mission creep. CIS felt that there was urgent need for further analysis and discussion into the appropriate (and inappropriate) uses of digital ID systems. Through research, we realised that the use of a Digital ID system is inextricably linked to the governance structure and fundamental attributes of the Digital ID system. Hence, a use analysis of Digital ID systems is best accomplished through an evaluation framework that provides principles against which Digital ID may be evaluated.

Consequently, the Evaluation Framework lays out a series of tests that can be used across jurisdictions to assess the legitimacy and governance of Digital ID. CIS selected three sets of tests – the Rule of Law tests, Rights-based tests, and Risks-based tests – to form the bedrock of the Evaluation Framework for Digital ID. CIS adopted the definition of 'digital identity' provided by David Birch, as a "system where identification (the process of establishing information about an individual), authentication (the process of asserting an identity previously established during identification) and authorisation (the process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity) are all performed digitally". Such a definition departs from the ID4D Practitioner's Guide that defines authorisation from the lens of eligibility, i.e. the process of determining whether a person is 'authorised' or 'eligible'.

In coming up with these tests, CIS adopted a first principles approach, drawing from methodologies used in documents such as the international Necessary & Proportionate Principles on the application of human rights to communication surveillance, the OECD Privacy Guidelines, and international scholarship on harms based approaches.

RULE OF LAW TESTS

Digital ID systems per se involve a vast collection of personal and sensitive personal data that infringe the privacy of individuals. Any such restriction on fundamental rights must be legal, backed by a legitimate aim, narrowly tailored in scope and application, accountable, and prevent mission creep. Hence, the Rule of Law tests evaluate whether a rule of law framework exists to govern the use of Digital ID and ensure sufficient deliberation before a Digital ID system is implemented for public and private actors. These tests ask six questions about:

1) **Legislative mandate** – whether the Digital ID project is backed by a validly enacted law, and whether the law amounts to excessive delegation.

2) **Legitimate aim** – whether the law has a validly defined legitimate aim.

3) **Actors and purpose** – whether the law clearly specifies the actors who use digital ID and the purposes for which the Digital ID is used.

4) **Grievance redress** – whether the law provides for adequate redressal mechanisms against actors who use the Digital ID and govern its use.

5) **Accountability** – whether there are adequate systems of accountability for all the (public and private) actors and users in the Digital ID system.

6) **Mission creep** – whether there is a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of Digital ID.

RIGHTS-BASED TESTS

Criticism of Digital ID systems focus on their violations of privacy – whether through the mandatory collection of sensitive personal data, risk of surveillance and profiling, or the lack of robust access control mechanisms – and the risk of exclusion. Hence, the Rights-based tests put forth certain rights-based principles, such as necessity and proportionality, data minimisation, access control, exclusion, and mandatory use that should be used to evaluate the extent to which the rights of citizens are being infringed through the use of Digital ID systems.

These tests ask five questions about:

1) **Necessity and proportionality** – whether the privacy violations arising from the use of Digital ID necessary and proportionate to achieve the legitimate aim.

2) **Data minimisation** – whether there are clear limitations on what data may be collected, how it may be processed, and how long it is retained for, during the use of Digital ID.

3) **Access control** – how is access by state and private actors to personal and sensitive personal data controlled through the law.

4) **Exclusion** – whether there are adequate mechanisms to ensure that the adoption of Digital ID does not exclude citizens/residents or restrict their access to benefits and services.

5) **Mandatory use** – whether there are valid legal grounds to justify the mandatory nature of Digital ID, if any.

RISK-BASED TESTS

A rights-based constitutional approach to evaluating Digital ID is necessary, but not sufficient, to ensure a well-functioning Digital ID system. Regulation of Digital ID must be sensitive to the different types of harms caused by its uses (such as privacy harms, exclusion harms, and discriminatory harms), the severity and likelihood of the harm, and must build in mitigation mechanisms to reduce the probability or impact of the harm. Although most countries do not perform such risk-based tests, CIS hopes that by incorporating these tests into the Evaluation Framework, governments will have a more realistic picture of the harms that are likely to occur in a Digital ID system and take appropriate steps to reduce the risk of the same. These tests ask five questions about:

1) **Risk assessment** – whether decisions regarding the legitimacy of uses, benefits of using Digital ID, and their impact on individual rights is informed by risk assessment.

2) **Differential risk approach** – whether the law adopts a differentiated approach to governing uses of Digital ID (such as per se harmful, per se not harmful, and sensitive), based on the risk factors.

3) **Proportionality** – whether the governance framework in the Digital ID law is proportional to the likelihood and severity of the possible risks of its use.

4) **Response to risks** – given certain demonstrably high risks from the use of Digital ID, whether the law has built in mitigatory mechanisms to restrict such use.

Using the Evaluation Framework, CIS published case studies on the use of Digital ID for the delivery of welfare, for verification, and in the health care sector. Country specific case studies were carried out for Estonia's e-Identity program, India's e-KYC framework, India's Unique Identity (Aadhaar) programme, and Kenya's Huduma Namba programme.

The eventual aim of the Evaluation Framework is to evolve these three tests into a set of best practices that can be used by policymakers when they create and implement Digital ID systems; provide guidance to civil society to evaluate the functioning of a Digital ID system; and highlight questions for further research on the subject. Through this project, in collaboration with RIA, we hope to fulfil some of these goals. ■