KICTANet
KENYA ICT ACTION NETWORK

Implementing Huduma Namba: Challenges and Prospects.

Executive Report, August 2020

Implementing Huduma Namba: Challenges and Prospects

August 2020

Published by: Kenya ICT Action Network (KICTAnet) with support from AccessNow.

Authors: Mutindi Muema, Angela Minayo and Tevin Mwenda
Edited by: Victor Kapiyo

ABOUT KICTAnet: The Kenya ICT Action Network (KICTAnet) is a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. The Network is a thought leader and is dedicated to bringing evidence, expertise, and more voices into ICT policy decision-making. KICTANet promotes public interest and rights based approach in ICT policy making.

Author:

Mutindi Muema, Tevin Mwenda
and Angela Minayo

Design & Layout:

MediaForce Communications
www.mfc.ke | @mfcafrica

September 2020

www.kictanet.or.ke

Table of Contents

List of Abbreviations

CEDAW	Convention on Elimination of all forms of Discrimination against Women
CRC	Convention on the Rights of the Child
CSO	Civil Society Organisation
DNA	Deoxyribonucleic Acid
DPA	Data Protection Act
ECOWAS	Economic Community of West African States
GPS	Global Positioning System
IBLF	International Business Leaders Forum
ICCPR	International Covenant on Civil and Political Rights
ICT	Information Communication and Technology
ID	Identification
ID4D	Identification for Development
IEBC	Independent Electoral and Boundaries Commission
IFC	International Finance Corporation
IPRS	Integrated Population Registration System
KES	Kenya Shillings
KRA	Kenya Revenue Authority
KIEMS	Kenya Integrated Election Management System
NHIF	National Hospital Insurance Fund
NSSF	National Social Security Fund
NIIMS	National Integrated Information Management System
NEMIS	National Education Management Information System.
NTSA	National Transport and Safety Authority
PIN	Personal Identification Number
RPA	Registration of Person Act
SDGs	Sustainable Development Goals
SIM	Subscriber Identity/Identification Module
UDHR	Universal Declaration of Human Rights
UN	United Nations

Executive Summary

On 31st December 2018, the President assented to the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 which came into force on 18th January 2019. Section 9A of the Act amended the Registration of Persons Act by establishing a National Integrated Identity Management System (NIIMS). NIIMS is intended to be the single source of personal information of all Kenyan citizens and foreigners residing in the country. The ambitious project, dubbed "Huduma Namba" loosely translated to service number, is the subject of this study.

This study provides the legal and historical context of Kenya's national identity management system. It also examines the transition to a digital system, through the Huduma Namba project, and its human rights impact and concerns.These concerns include: the adequacy of public participation, adequacy of data protection, exclusion from access to socio-economic rights and discrimination of existing minority groups. In addition, the study highlights three countries with experience of using digital identity systems as case studies. Finally, the study provides key recommendations to stakeholders.

The methodology for this study is guided by the Human Rights Impact Assessment approach as advanced by the International Business Leaders Forum (IBLF) and the International Finance Corporation (IFC), in association with the UN Global Compact. This is a mixed approach where the researchers gathered data on the legal and human rights concerns raised by the Huduma Namba as well as insights from a consultative meeting with stakeholders.

Our findings show that there exists serious data protection concerns regarding the technical design and legal framework for NIIMS. Secondly, Huduma Namba carries the risk of excluding minorities from accessing government services. These essential services directly impact the right to equality and freedom from discrimination, freedom of association, political rights, freedom of movement and residence, labour relations, the right to property. Third, the government has not specifically addressed the rights of children in relation to the collection and integrity of their data. Fourth, the government is yet to promulgate enforceable and sufficient data protection regulations that would apply to Huduma Namaba data.

Despite the identified issues, all is not lost.The study found a variety of best practices on national digital identities from the United States of America, Estonia and India. Additionally, there are international standards on digital identity such as the World Economic Forum Emerging Best Practices which advocates for digital identity to be fit for purpose, inclusive, useful, secure and offer choice to registrants.

The experience from Estonia regarding blockchain, cryptography and back-up measures in case of a data breach is vital. India's experience points to the challenges such as duplication in registration, data breaches and inflated numbers. Borrowing from the wisdom of the Indian Supreme Court on India's Aadhaar case, Huduma Namba should not restrict access to essential government services such as education and healthcare.

In conclusion, the study recommends measures that can safeguard compliance with data protection principles and respect for human rights in the use of Huduma Namba in Kenya as well as key points for multi stakeholder engagement across Parliament, Executive, the private sector, civil society organisations, citizens, media, the technical community and academia.

Introduction

1.0

1.1 Background

According to the World Bank, there are over 1 billion people in the world without legal Identification, and close to half of them live in sub-Saharan Africa[1]. This makes the provision of legal identity a key priority particularly for countries in sub-Saharan Africa, such as Kenya

Legal Identity is important as it enables people to access basic and critical services from both private and public entities[2] The obligation to facilitate 'access to service' is what guided the government to develop a digital identification program through the establishment of the National Integrated Information Management System (NIIMS). The project, popularly known as 'Huduma Namba' is expected to enhance access to Government services for persons in Kenya.[3] .

All global efforts towards digital identification cards, systems and programs are rooted in the right to personal identity, which stems from the right to life. Globally, the human right to life is enshrined in the 1948 Universal Declaration of Human Rights (UDHR). The UDHR is domesticated in many constitutions of nations across the globe including in Kenya.

1.2 Context

In September 2015, world leaders at the historic United Nations (UN) Sustainable Development Summit, adopted the new 2030 Agenda for Sustainable Development, including the 17 Sustainable Development Goals (SDGs).[4]. The SDGs officially came into force on 1 January 2016, with new goals that universally apply to all. The SDGs require countries to mobilize efforts over a fifteen year period to end all forms of poverty, fight inequalities and tackle climate change, while ensuring that no one is left behind. SDG 16 requires all nations to promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels. This includes providing legal identity for all, including birth registration by 2030.[5] It is particularly important as about 1 billion people are legally 'invisible' because they cannot prove who they are.[6] This number includes an estimated 625 million children under 14 years, whose births were never registered. Part of this 'invisible' population is hosted in Kenya[7] and the developments at UN level are part of what led the government to NIIMS.

---

1 Identification for Development," last modified May 17, 2020, https://id4d.worldbank.org/global-dataset/visualization

2 Ibid

3 Huduma Namba, last accessed on August 4, 2020, https://www.hudumanamba.go.ke/

4 Background of the Sustainable Development Goals, last accessed on June 28, 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals/background/

5 "Sustainable development goals," last modified May 10, 2020, https://sustainabledevelopment.un.org/sdg16

6 "Goal 16 Peace, justice and strong institutions," last modified May 10, 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals/goal-16-peace-justice-and-strong-institutions.html

7 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

Globally, one of the most robust programs supporting SDG 16 is the Identification for Development Program, a World Bank project that assists countries to develop digital identification systems.[8] The World Bank assists by conducting assessments of the country's identity ecosystem using the Guidelines for Identification for Development (ID4D) Diagnostics, providing technical and advisory services to the country, providing financial assistance and monitoring the process after implementation.[9] The World Bank is currently working with the Economic Community of West African States (ECOWAS) Block and Countries like Morocco in creating digital National Population registers.[10]

1.3 Methodology

This study reviews Kenya's journey towards a digital ID system from a human right's perspective. The review is guided by the Human Rights Impact Assessment approach as advanced by the International Business Leaders Forum (IBLF) and the International Finance Corporation (IFC), in association with the UN Global Compact.

The study uses a mixed approach. The research commenced with a desktop review of relevant literature, policies, laws, regulations, cases, reports and other documents from Kenya,and other relevant jurisdictions. A consultative meeting was thereafter convened and focus group discussions were conducted with several representatives from government, industry, civil society, media and academia in August 2020. All the information collected was analyzed and forms the basis of this study.

8 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

9 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

10 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020


huduma
KENYA
service excellence
1234 5678 9876
VALID
THRU 02/19
,YA W
470254

The making of Huduma Numba

2.0

2.1 History of Legal Identification in Kenya

The first form of government identification in Kenya was the issuance of Identification Cards also known as Kipande.[11] This began in 1915 with the passing of the The Native Registration Ordinance.[12] The purpose of identification was to create an instrument to control and regulate the recruitment of African males into the colonial labour force.[13]

In 1947, the Kipande was replaced by an Identity card which had fingerprints. The Registration of Persons Ordinance made it mandatory for all male persons of all races above the age of 16 years to be registered[14]. Under this law, the ID cards issued distinguished between protectorate and non-protectorate persons. Although the Ordinance sought to elimitate discrimination based on race, it retained gender-based discrimination. The trend continued even after independence until 1978 with the introduction of the Registration of Persons Act (Cap 107, Laws of Kenya) which required the registration of women above the age of 16 years. A further amendment to the Act was made in 1980 raised the minimum age of registration from 16 to 18 years.

In 1995, the first generation ID cards were replaced by the second generation ID cards.[15] These ID cards were smaller, laminated and contained basic information such as name, sex, date, place of birth, place of orignin, and date and place of issue.[16] It also added the 8 digital national ID number as well as a 9 digit serial number. These cards have since been upgraded to the current plastic cards without fundamentally changing the information appearing on the card.[17] The information at the front of the card is machine readable.[18]

11 Identification for Development," last modified May 17, 2020, https://id4d.worldbank.org/global-dataset/visualization

12 Ibid

13 Huduma Namba, last accessed on August 4, 2020, https://www.hudumanamba.go.ke/

14 Background of the Sustainable Development Goals, last accessed on June 28, 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals/background/

15 "Sustainable development goals," last modified May 10, 2020, https://sustainabledevelopment.un.org/sdg16

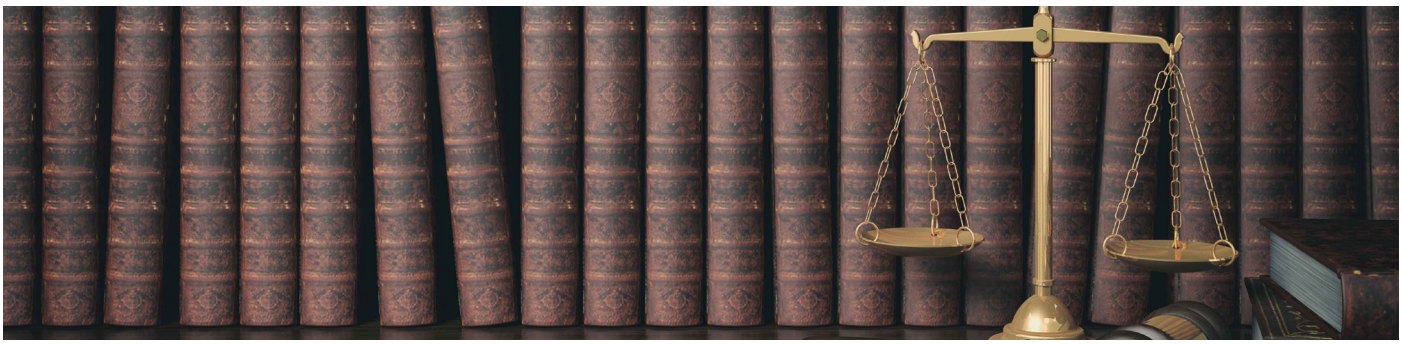
16 "Goal 16 Peace, justice and strong institutions," last modified May 10, 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals/goal-16-peace-justice-and-strong-institutions.html

17 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

18 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

The 8 digital national ID number forms the basic reference for official identification and several other forms of registration for public and private services in Kenya including citizen applications for passports, driving license applications, political party membership, marriage solemnization and registration, access to online Government services on e-Citizen, company incorporation, pension registration, taxpayer registration, registration for National Social Security Fund and National Health and Insurance Fund, employee on boarding (to prevent child-labor), registration to professional membership associations, insurance services, financial and banking service, capital market trading accounts, device warranty redemption, participation in betting lotteries & gaming activities, among others.

The physical national ID card number is required for the issuance of telephone numbers, voter registration and voting as well as to access government buildings and a number of privately owned buildings and office premises. The physical ID card is also required for the purchase of items such as alcohol, real and movable property as well as the registration of some intellectual property rights. In many ways, access to premises and services, ownership of property as well as the enjoyment and preservation of human rights for adults in Kenya revolve around an individual's official identification through the national ID card.



2.2 Policy and Legislative Environment for Digital ID in Kenya

2.2.1 International Policy and Legal Framework

A number of international human rights instruments highlight the importance of the right to a nationality. These include the following:

a) The Universal Declaration of Human Rights (UDHR) in Article 15 provides that everyone has a right to a nationality and prohibits arbitrary deprivation of nationality.

b) The International Covenant on Civil and Political Rights (ICCPR) in Articles 24 and 25 respectively provide that all children have a right to a nationality and citizens the right to vote.

c) The Convention on Elimination of all forms of Discrimination against Women (CEDAW) in Article 9 guarantees women an equal right with men in respect to the nationality of their children.

d) The Convention on the Rights of the Child (CRC) in Articles 7 and 8 provide for the rights of children to acquire a nationality and prohibits the illegal deprivation of their identity.

The African Charter on Human and Peoples' Rights in Article 5, provides for the right to the recognition of a person's legal status. Nationality is an important part of identity. It is the legal bond that guarantees individuals the full enjoyment of all human rights as members of the political community. Although states maintain the sovereign right to regulate nationality, states' discretion is limited by international human rights standards that protect individuals against arbitrary state actions.[19] This is particularly relevant with regard to the rights to privacy, non- discrimination and equality before the law as well as accesses to civil and political rights.

2.2.2 Policy and Legislative Environment for Digital ID in Kenya

In Kenya, the legislative environment for legal and digital identity is anchored in the Bill of Rights under the Constitution of Kenya 2010. Article 53 provides for the right of a child to a name and nationality from birth. Article 12 provides for the right of a citizen to state issued documents of identification or registration.

vArticle 18 requires Parliament to enact legislation to govern the procedures for the acquisition of citizenship, the entry of persons into Kenya as well as the recognition of permanent or temporary residence status.

The Bill of Rights embodies Kenya's international human rights obligations. The following statutes directly govern the identification of persons in Kenya:
a) Age of Majority Act Cap 33 provides eighteen years as the general age of majority;

b) Births and Deaths Registration Act Cap 141 provides for the notification and registration of all births and deaths;

c) Registration of Persons Act Cap 107 - provides for the registration of persons and for the issuance of national identity cards;

d) Kenya Citizens and Foreign Nationals Management Service Act 2011 - establishes the Kenya Citizens and Foreign Nationals Management Service as well a national population register to support the administration of the laws relating to births and deaths, identification and registration of citizens, immigration and refugees, and the Integrated Population Registration System (IPRS).

e) Kenya Citizenship and Immigration Act,2011 - provides for matters relating to citizenship, issuance of travel documents (temporary passes and passports), immigration and connected purposes.

f) Kenya Revenue Authority Act,1995 - establishes the Kenya Revenue Authority as a central body for the assessment and collection of revenue, provides for Personal Identification Number (PIN) registration and issuance to ease administration and enforcement of the revenue laws.

g) National Hospital Insurance Fund Act,1998 – establishes the National Hospital Insurance Fund and provides for contributions to the fund and payment of benefits out of the fund.

19 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

h) National Social Security Fund Act, 2013 – establishes the National Social Security Fund, and provides for contributions to the fund and payment of benefits from the fund;

i) National Transport and Safety Authority Act 2012 - provides for the establishment of the National Transport and Safety Authority (NTSA), registration for, issuance and renewal of driving licenses as well as the registration of motor vehicles.

j) Basic Education Act & the Kenya National Examinations Council, 2012 provide for the registration of students for exams and forming the legal ecosystem for use of the National Education Management Information System (NEMIS).

k) Higher Education Loans Board Act, 1995 - provides for the registration of students in higher education institutions for financial aid purposes.

l) Independent Electoral and Boundaries Commission, 2011 - provides for voter registration and the conduct of national elections.

Each of these provide a unique legal identity to persons in Kenya. It is this multiplicity of legal identities that the government sought to do away with by creating a single source of truth - a new digital identity dubbed Huduma Namba to replace all the above.[20]
The Kenya Information and Communication Act as well as the Computer Misuse And Cybercrimes, 2018 provide in part for the protection of digital identities while the Data Protection Act, 2019 provides for the protection of personally identifiable information including legal and digital identities.

There are other laws that require use or production of IDs for access to services, products or premises. For example, the Private Security Regulation Act 2016 requires production of ID cards as a condition for access to premises, the Alcoholic Drinks Control Act 2010 and the Tobacco Control Act restrict sale and consumption of alcohol and tobacco to persons over the age of majority, while the Betting, Lotteries And Gaming Act Cap 131 restricts gaming and betting activities to persons over the age of majority.

2.2.3 Identification in Kenya

The Registration of Persons Act (RPA) requires all Kenyan citizens upon attaining the age of eighteen to obtain a national identification card.[21] Under the law, the National Registration Bureau is tasked with collecting all biometric and biographic information and issuance of national IDs.[22] In 2005, the head of the Public Service appointed an Inter-Ministerial Taskforce on the Integrated Population Registration System (IPRS).[23] The taskforce recommended the introduction of a unique personal

20 Africa's Invisible Millions Survive Without ID Documents, last modified August 6, 2020

21 "Registration of Persons Act Chapter 107,"last modified May 15, 2020, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/RegistrationofPersonsActCap.%20107.pdf

22 Department of Immigration Services," last modified May 15, 2020 https://www.immigration.go.ke/national-registration-bureau/

23 "Toa Kitambulisho! Evolution of Registration of Persons in Kenya," last modified May 10, 2020, https://www.theelephant.info/data-stories/2019/06/14/toa-kitambulisho-evolution-of-registration-of-persons-in-kenya/?print=pdf

identity number to be assigned to every citizen immediately they were born.[24]

According to the Kenya Law Reform Commission, the recommendations of this taskforce led to the establishment of the Integrated Population Registration System (IPRS) in order to create a harmonized approach to address the challenges encountered during registration of persons in Kenya.[25] The IPRS consolidated information obtained from the Civil Registration Department, National Registration Bureau and the Department of Immigration Service.[26]

The IPRS was set up by the government as a central database, containing data from several State agencies and giving a comprehensive view of an individual. The IPRS database shows an individual's birth certificate details, identity card details, academic certificates, NHIF and NSSF details together with an individual's Kenya Revenue Authority and Personal Identification Number all at the click of a button.[27]
IPRS data is available for access by third parties for the purpose of verification of details concerning an individual or for any other purpose as approved in writing by the Cabinet Secretary for Interior and Coordination of National Government. Each database query is charged at KES 5.00 providing an income stream for the government.[28] However, government agencies do not pay to access the population register.

The Cabinet Secretary may, on the advice of the Director of the Integrated Population Registration Service, enter into an agreement with a person for the provision of information from the IPRS on such terms and conditions relating to use, confidentiality, period and nature of access to the information and terms of payment, as he may consider appropriate. Firms like those in online banking and e-commerce use the IPRS to verify individuals' identity and credit history. Some employers also use the database to verify the academic credentials of those they are hiring.

IPRS had by January 2016 captured details of 35 million Kenyans from birth through their adult life.[29] According to the Ministry of Interior, the IPRS was built to provide a fool proof database that could be used to guard against identity theft.

2.2.4 Shortcomings of the IPRS

According to the Kenya Law Reform Commission,[30] there were fundamental challenges to the Kenyan Identification systems that remained unresolved despite the encouraging steps made under IPRS. These included: an individual's data was still being collected by multiple government agencies resulting in inefficiency and continued wastage of resources. In some cases, data being integrated into IPRS

24 "The Bliss of NIIMS Paradise: The Legal Context of the Huduma Namba," last modified May 10, 2020, http://www.klrc.go.ke/index.php/klrc-blog/645-the-bliss-of-niims-paradise-the-legal-context-for-the-huduma-namba

25 "Toa Kitambulisho! Evolution of Registration of Persons in Kenya," last modified May 10, 2020, https://www.theelephant.info/data-stories/2019/06/14/toa-kitambulisho-evolution-of-registration-of-persons-in-kenya/?print=pdf

26 Ibid

27 "Interior CS sets terms for accessing details on individuals," last modified May 10, 2020, https://www.businessdailyafrica.com/news/Interior-CS-sets-terms-for-accessing-details-on-individuals/539546-3217642-wrk3v0z/index.html

28 Ibid

29 Ibid

30 "The bliss of NIIMS Paradise: The Legal Context of the Huduma Namba," last modified May 10, 2020, http://www.klrc.go.ke/index.php/klrc-blog/645-the-bliss-of-niims-paradise-the-legal-context-for-the-huduma-namba

contained inaccuracies, necessitating recollection of personal information from the sources. Also, in some cases information relating to children was not being captured comprehensively at birth. For example, in 2017, the Civil Registration Service registered 61% of births after registration the details were required to enroll for exams. It had been the ambition of the government to attain 100% registration of births by, among other means, employing suitable technology.

The IPRS failed to constitute a master register which could be regarded as "a single source of truth" as it relied on information from multiple sources some of which conflicted. For example, it is not uncommon for the same person to have a different name in a passport, in the national identification card and birth certificate. Such issues dilute the credibility of IPRS as the integrated national registration system. Further, the multiple registration regimes issued several identity documents. Kenyans are then compelled to obtain, keep and move around with multiple identification documents such as Identity Cards, Passports, Driving Licences, NSSF and NHIF cards, 'inconveniencing' them. The question evaluated by the government has been, why not have only one card? Or should one even have a card, where just a number can suffice?
The highlighted IPRS shortcomings led to the proposal and formation of the National Integrated Information Management System (NIIMS) [31] dubbed Huduma Namba project. In order to improve and build upon the progress made by IPRS, the Government initiated NIIMS programme under Executive Order No. 1 of 2018. NIIMS was subsequently approved by the National Assembly via the Statute (Miscellaneous Amendment) Act, No 19 of 2018.

2.2.5 National Integrated Information Management System (Huduma Namba)

The NIIMS National Integrated Information Management System is a system designed by the Kenyan Government to create and manage a central master population database as the 'single source of truth' on a person's identity.[32] The database will contain information of all Kenyan citizens and foreign nationals residing in Kenya and will serve as a reference point for ease of service delivery to the people of Kenya and the people in Kenya.[33]

The government cited several justifications for establishment of NIIMS including:

- The current manual persons' databases left the country vulnerable to various emerging security threats.[34]

- The current identification systems were outdated and were being exploited by criminals who are using them to commit fraud and massive forgery.[35]

- Criminal aliens living in Kenya were colluding with immigration officers to get

31 Ibid

32 Ibid

33 "Brochure National Integrated Identity Management System (NIIMS)," last modified May 10, 2020, https://www.huduma-namba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

34 Ibid

35 Ibid

Kenyan documents.[36]

On 20th November 2018, the National Assembly enacted the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018. The President assented to the Act on 31st December 2018, and it came into force on 18th January 2019. The effect of the Act was to amend several provisions of a number of existing statutes, among them the Registration of Persons Act. The amendments to the Registration of Persons Act establish the National Integrated Identity Management System (hereinafter "NIIMS") intended to be a single source of personal information of all Kenyan citizens as well as foreigners' resident in Kenya. The amendment was promulgated as set out below:

9A Establishment of the National Integrated Identity Management Sytems

(1) There is established a National Integrated Identity Management System.

(2)The functions of the system are —

(a) to create, manage, maintain and operate a national population register as a single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya;

(b) To assign a unique national identification number to every person registered in the register;

(c) To harmonise, incorporate and collate into the register, information from other databases in Government agencies relating to registration of persons;

(d) To support the printing and distribution for collection of all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel documentation, student identification cards issued unvder the Births and Deaths Registration Act, Basic Education Act, Registration of Persons Act, Refugees Act, Traffic Act and the Kenya Citizenship and Immigration Act and all other forms of government issued identification documentation as may be specified by gazette notice by the Cabinet Secretary;

capture the various forms of information contained in the identification documents in paragraph (d) for purposes of issuance of a single document where applicable;

(e) To prescribe, in consultation with the various relevant issuing authorities, a format of identification document to

(f) To verify and authenticate information relating to the registration and identification of persons;

(g) To collate information obtained under this Act and reproduce it as may be required, from time to time;

(h) To ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register;

(i) To correct errors in registration details, if so required by a person or on its own initiative to ensure that the information is accurate, complete, up to date and not misleading; and

(j) To perform such other duties which are necessary or expedient for the discharge of functions under this Act.

36 Ibid

(3) The Principal Secretary shall be responsible for the administration, coordination and management of the system.

NIIMS would therefore harmonize all citizen and alien information and help the government to offer services efficiently as well as reduce duplication of information.[37]

The government stated it would implement NIIMS in 3 phases:[38]

Phase 1

Mass registration of persons within the territory of Kenya with the key identifier as birth certificate, ID card number and passport or alien card number for foreigners;

Phase 2

Verification and authentication of data provided

Phase 3

Issuance of Huduma Namba and huduma cards.

In phase 1 of mass registration, the government targeted to register over 40 million people on NIIMS.[39] It conducted a countrywide registration campaign led by President Uhuru Kenyatta from March to May 2019. By the time the registration ended the government had managed to register 36 Million people on NIIMS.[40]

Expected Huduma registration target

40 million

Attained Huduma registration

36 million

The requirements for registration were as follows:

- Filled-in Huduma Namba registration form;
- Original Identification Card for a Kenyan citizen above 18 years old;
- Original birth certificate for Kenyans below 18 years old;
- Original passports or alien cards for foreign residents;
- Place of birth;
- Disability registration number;
- National Hospital Insurance Fund (NHIF) number;
- National Social Security Fund (NSSF) number;

37 Ibid

38 "Huduma Namba Frequently Asked Questions,"last modified May 10, 2020, http://www.hudumanamba.go.ke/faqs/

39 "36 million registered for Huduma Namba," last modified May 15,2020, https://www.the-star.co.ke/news/2019-05-24-36-million-registered-for-huduma-namba/

40 Ibid

- Passport number and expiry date;
- Birth Certificate Entry number;
- Driver's license number;
- Kenya Revenue Authority (KRA) Personal Identification Number (PIN);
- Marital status and spouse(s) name(s) and their national IDs andPassport numbers;
- Names of parents or guardians and their national IDs and Passport numbers;
- Permanent and current address;
- Contact details; and,
- National Education Management Information System (NEMIS) number.

Those who did not have the required documents were required to present themselves to the NIIMS registration officers for further guidance. The government stated that registration would continue at chief's camps after the lapse of the deadline of May 24th 2019.[41] It further announced that another round of registration would be conducted, however the exact date was not given.[42]

In relation to the Huduma Namba cards, the government stated in January 2020 that the issuance of the cards would start once the High Court allowed the project to continue.[43] On January 30th 2020, the High Court however halted all further implementation of NIIMS until the government enacted a proper data protection framework.[44] The government is currently in the process of developing data protection regulations applicable to NIIMS. The proposed regulations are currently undergoing public participation.

41 Ibid

42 "State to roll out second phase of Huduma Namba listing," last modified May 12, 2020, https://www.standardmedia.co.ke/article/2001358715/state-to-roll-out-second-phase-of-huduma-namba-listing

43 "Issuance of Huduma Namba cards to begin - Oguna," last modified May 12 2020 https://www.the-star.co.ke/news/2020-01-31-issuance-of-huduma-namba-cards-to-begin-oguna/

44 "Nubian Rights Forum & 2 others v Attorney General & 9 others (Interested Parties) [2020] eKLR," last modified May 15, 2020, http://kenyalaw.org/caselaw/cases/view/189189/


huduma
KENYA
1710 0002 4552
MasterCard

Concers on Huduma Namba

3.0

3.1 Policy and legislative gaps

When the Government announced the Huduma Namba project, a number of Human Rights groups, and registered societies challenged the legality of the project by filing a court case. The groups cited the government's actions as putting the cart before the horse by rolling out NIIMS registration without a proper legal framework in place. Further, that necessary legal protections to ensure individual privacy, cybersecurity, sufficient public participation and non-discrimination, inclusivity and equality in access to government services were lacking.

The Case, Nubian Rights Forum & 2 others v Attorney General & 9 others (Huduma Namba case)[45] raised awareness of the existing policy and legislative gaps present at the roll out and during the implementation of Phase I of the Huduma Namba project. The case questioned: the constitutionality of NIIMS; the use of a Miscellaneous Amendments Bill to pass substantive amendments to the Registration of Persons Act instead of following proper procedure for introduction of substantive amendments; the lack of sufficient public participation in the process introducing Huduma Namba that would radically shift the manner in which citizens and residents access Government services; inadequate legal and policy frameworks to guarantee data privacy and protection of personally identifiable and sensitive information; as well as,the risk that NIIMS could further entrench discrimination and exclusion of marginalized groups in Kenya.[46]

The Petitioners requested the High Court to suspend the commencement of the Huduma Namba roll out. In the initial ruling issued by the High Court on 1st April 2019,[47] right before the Huduma Namba roll out on 2nd April 2019, allowed the government to proceed with phase I roll out but was expressly prohibited from: linking Huduma Namba to access or provision of government services; requiring mandatory registration of Kenyan citizens or residents; collecting DNA samples or GPS coordinates of registrants; and, setting any deadline for registration, or sharing

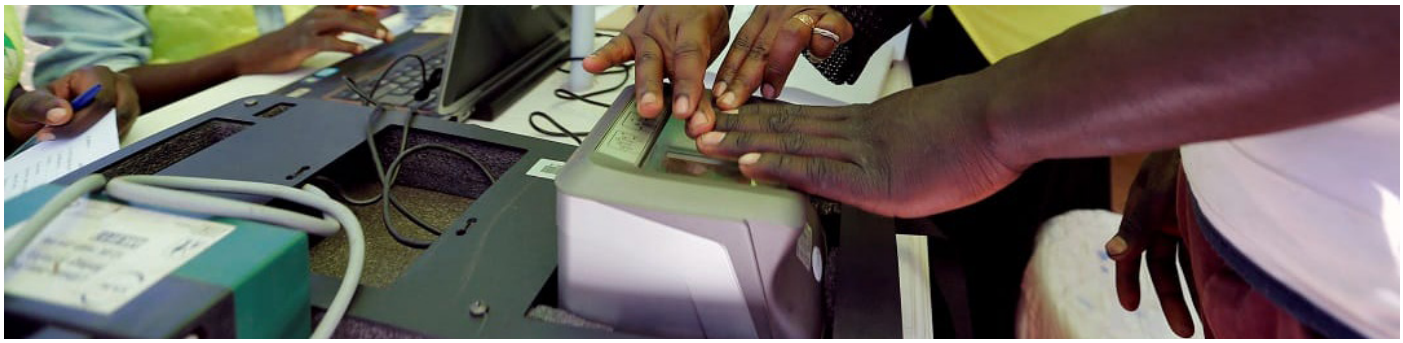
45 "Nubian Rights Forum & 2 others v Attorney General & 9 others (Interested Parties) [2020] eKLR,"

46 "KHRC Huduma Namba Stopped," last modified May 15, 2020, https://www.khrc.or.ke/2015-03-04-10-37-01/press-releases/704-press-release-huduma-namba-stopped.html

47 "Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2019] eKLR," last modified 28th June 2020, http://kenyalaw.org/caselaw/cases/view/172447/

the data collected with third parties.[48]

On 30th January 2020 the High Court delivered its final judgment and findings in the case.[49] We highlight the court findings below as we discuss the policy and human right concerns surrounding the Huduma Namba roll out.



3.2 Public Participation

NIIMS was introduced on 31st December 2018 by section 9A of the Statute Law Miscellaneous (Amendment) Act No. 18 of 2018,[50] an omnibus bill containing amendments to several Acts of Parliament. Consequently, it was debated in the National Assembly in August 2018, without proper publicity or public understanding of the implications of the proposed establishment of NIIMS. This later raised questions about whether NIIMS was established with input from members of the public and interested groups as required under Article 10 and 118 of the Constitution of Kenya, 2010. Further, questions arose whether the Bill was a Bill that touched on Counties and if it should have been reviewed and debated by the Senate.[51]

These concerns were raised in the Huduma Case and the High Court found that there was adequate public participation on the Bill promulgated to establish NIIMS notwithstanding the fact that it was an omnibus Bill. The Court also found that the Bill did not need to go to the Senate for approval as the establishment of NIIMS did not through a point of order raised by Hon. Otiende Omollo but went ignored. All in all, the manner in which the amendments were introduced escaped public scrutiny and did not result in early stage engagemen touch on counties as the proposed registry is national, and not county based.[52]

Moreover, other than publication of the list of the statutes to be amended and interagency efforts within government for the adoption of NIIMS, the public and

48 "KHRC Huduma Namba Stopped,"

49 "Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR,"http://kenyalaw.org/caselaw/cases/view/189189/

50 http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf

51 "Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2019] eKLR," last modified 28th June 2020, http://kenyalaw.org/caselaw/cases/view/172447/

52 KHRC, " Huduma Namba Stopped," https://www.khrc.or.ke/2015-03-04-10-37-01/press-releases/704-press-release-huduma-namba-stopped.html#:~:text=In%20April%202019%2C%20the%20High,the%20Huduma%20Namba%20enrollment%20exercise.

several human rights organizations appeared not to be aware of the proposed Huduma Namba project until Government's mass communication campaigns in early 2019 ahead of phase I roll out.

Ideally, given the far-reaching effects of the establishment of NIIMS on fundamental human rights, a substantive bill specifically dedicated to NIIMS would have been more appropriate. This concern was also shared in the National Assembly on 28th August 2018

In July 2019, and as a result of the public participation concerns raised by the petitioners in the Huduma Case, the Government published a draft Huduma Bill[53] and convened one public participation forum in Nairobi,[54] where the public was allowed to submit comments on the Huduma Namba project by 5th August 2019.[55] The draft Huduma Bill was however abandoned and did not proceed to Parliament with no further amendments made as a result of the public participation window that ended on 5th August 2019.

The above point to the need for clear guidelines on public participation thresholds particularly in relation to the use of omnibus bills to make amendments that substantially affect one or more human rights. Although the High Court in the Huduma Namba case found that there was 'adequate public participation', the concerns raised by Hon. Otinde Omollo in Parliament, concerns by the Petitioners in the Huduma Case as well as government publishing a draft Huduma Bill all point to the need for definition on what amounts to sufficient public participation. This needs to be addressed, particularly in relation to the use of omnibus Bills to make amendments that substantially affect one or more human rights.

3.3 Right to Privacy

There are various privacy concerns with regard to the establishment and implementation of NIIMS. This section outlines the various issues stemming from the constitutional right to Privacy. It is important to note that the Data Protection Act was enacted in November 2019 to provide a legislative framework for the operationalization of Article 31. The Right to Privacy is enshrined in Article 31 of the Constitution of Kenya 2010.

53 "The Huduma Bill 2019," last modified May 10, 2020, https://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf

54 "Public Participation on the Huduma Bill 2019," May 10, 2020, https://www.hudumanamba.go.ke/wp-content/uploads/2019/07/Huduma-Bill-Call-for-Public-Participation.pdf

55 "Public Participation on the Huduma Bill 2019,"

Every person has the right to privacy, which includes the right not to have—

Their person, home or property searched;

Their possessions seized

Information relating to their family or private affairs unnecessarily required or revealed

the privacy of their communications infringed.

The Article provides that:
Data protection issues are categorized as privacy concerns for purposes of this study. Information security concerns are also categorized as privacy concerns as information security protocols and technologies help secure the privacy and integrity of personal data, guarding against infringement of privacy and unnecessarily revelation. The key privacy concerns related to NIIMS are highlighted below.

3.3.1 Exclusion of NIIMS from the Data Protection Act

When NIIMS was rolled out, Kenya did not have a substantive data protection law or policy. However, and at the time, two Data Protection Bills, 2018 were nonetheless being discussed in the Senate and the National Assembly. The lack of an enforceable data protection law raised various concerns regarding the legal framework guiding the establishment of NIIMS.

In November 2019, the Data Protection Act (DPA) was assented into law. Although the Act provides a framework for data protection including data protection principles, data subject rights and government privacy obligations, it specifically excluded the Registration of Persons Act from its scope. The DPA provides

51 (2) The processing of personal data is exempt from the provisions of this Act if —

(a) it relates to processing of personal data by an individual in the course of a purely personal or household activity;

(b) if it is necessary for national security or public interest; or

(c) disclosure is required by or under any written law or by an order of the court.

54. The Data Commissioner may prescribe other instances where compliance with certain provisions of this Act may be exempted.

NIIMS is established under the RPA and housed under the Ministry of Interior and Coordination of National Government, which is responsible for national security.[56] Part of the justifications by the Government for the establishment of NIIMS include public interest and national security concerns. Further, the initial draft of the Data Protection Bill,specifically provided for application of the Act to the Registration of Persons Act through consequential amendments in Schedule II.[57] However, this provision was deleted, and section 51 (2)(b) specifically excludes NIIMS from the application of the Data Protection Act based on national security.

It is a risky exercise for the Government to establish a system solely relying on personal and sensitive data including biometrics, GPS and DNA, in the absence of an applicable and enforceable data protection framework. A secure and reliable digital identity system needed to be anchored on a strong data protection framework in order to ensure the protection of privacy, data integrity, purposeful use, the prevention and criminalization of unlawful access of the collected personal data.

The lack of data protection laws and policies expressly applicable to NIIMS was raised in the Huduma Case and the Court found that even with the enactment of the Data protection Act, the legal safeguards and data protection frameworks for NIIMS were inadequate as the Registration of Persons Act (establishing NIIMS) is not one of the Acts to which the Data Protections Act applies. The Court noted the RPA's exclusion from Schedule I on consequential amendments excluded NIIMS from the ambit of the Data Protection Act even though the Act legislates on personal identifiable information such as biometrics and DNA and other identifiers collected under enrolment into NIIMS.

The Court also found that there is a legal gap caused by the lack of regulations for operationalization of the Data Protection Act and particularly, the lack of regulations outlining circumstances when the Data Commissioner may exempt people or systems from the application of the Act. The regulatory framework also lacks data sharing codes on the exchange of personal data between government departments. These regulations are necessary, as they will have implications on the protection and security of personal data. The Court found that adequate protection of the data collected under NIIMS requires the operationalization of the Data Protection Act and regulations outlining its application to NIIMS.

3.3.2 Collection of Excessive Personal Information

The Statute Law Miscellaneous (Amendment) Act No. 18 of 2018, provided for the collection of sensitive personal data including biometric and Global Positioning System (GPS) information. Under the Act:

56 "Huduma Number Organizational Structure," last modified May 11, 2020, http://www.hudumanamba.go.ke/organogram/

57 "The Data Protection Bill 2018," last modified May 11, 2020, https://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf

"sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject;

"Biometric" means unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form.

"Global Positioning System coordinates" means the unique identifier of precise geographic location on the earth, expressed in alphanumeric character being a combination of latitude and longitude.

The collection of biometric and GPS information that would form part of the NIIMS database amounts to collection of excessive and intrusive personal information. Under the Act: However, theCourt in the Huduma Namba case found that the personal information collected by the Government was not excessive, intrusive or disproportionate with regard to the collection of biometric information (save DNA) and the requirement for collection of biometrics did not violate the individual right to privacy.[58]

The biometrics it held, were necessary to enable the integration of all existing government databases (IPRS, ID, NHIF, NSSF, KRA PIN, Passport numbers etc.) and the government had proved that biometrics were an integral part of NIIMS and the establishment of NIIMS was in the interest of the public.

The Court further ruled that DNA and GPS collection was not authorized or specifically anchored in empowering legislation and thus any such collection is unconstitutional and a violation of Article 31 of the Constitution. The proposed collection of DNA and GPS coordinates by the Government for purposes of identification was found to be both intrusive and unnecessary.

3.3.3 Risks to Information Security

Idemia parliamentary ban and association with previous data leaks

On 12th October 2018, the Ministry of Interior Affairs and Coordination of National Government conducted the procurement process of biometric kits for implementation of NIIMS.[59] In late 2018, IDEMIA (previously known as Morpho, OT-Morpho, Safran Identity and Security) supplied 31,000 biometric kits to register and enroll persons under(NIIMS).[60] The contract cost taxpayers Ksh. 6 billion (60 Million USD).

58 "Nubian Rights Forum & 2 others v Attorney General & 9 others (Interested Parties) [2020] eKLR"

59 National Integrated Identity Management System (NIIMS) Brochure, last modified May 11 2020, http://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf

60 "Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2019] eKLR," para. 419, last modified 28th June 2020, http://kenyalaw.org/caselaw/cases/view/172447/

The same company had been contracted to develop the voter registration system in the 2017 General Election known as Kenya Integrated Election Management System (KIEMS) whose data was compromised.[61] The company also supplied biometric voter registration kits in 2013.[62]

In 2017, the firm supplied 45,000 biometric authentication kits which were used in the Kenya General Elections.[63] The 2017 elections were marred with irregularities and suspicion that the election results were compromised.[64] From the government's response in the Huduma Case, the same kits were cleaned and reused for the NIIMS Huduma Namba registration process,[65] resurrecting concerns regarding the security and integrity of data collected and stored using Idemia technologies.

Due to the compromise and leak of KIEMS data, multiple unexplained incidences of company rebranding within a short time frame as well as the infringement of the requirements of the Companies Act 2015 by Idemia, MPs called for blacklisting of the firm from doing business with the government.[66] On 23rd April 2019, the firm was handed a ten-year ban from government contracts by parliament.[67]

Further, the Kenyan government claims that NIIMS will prevent the duplication of personal data and will be the single source of truth for anyone wishing to access government services. In the Huduma Namba case one of the expert witnesses highlighted the fact that NIIMS might not solve the duplication problem since NIIMS has been heavily borrowed from the Indian Aadhaar system.[68] In India, it was found that digital identity is not the complete answer in avoiding de-duplication as it still exists and a study conducted found that up to 10 million people would be affected with Duplication.[69] There is a high probability this will be the case with NIIMS especially since NIIMS uses the same OT Morpho algorithms as Aadhaar. This raises questions regarding how the government will avoid duplication in Kenya especially if they are to rely on Huduma Numba as the single source of truth for people's identity.

---

61 "MP Wants IDEMIA Banned From Doing Business in Kenya," last modified May 11, 2020, https://www.nation.co.ke/news/French-IT-firm-in-trouble-over-KIEMS-kits-tender/1056-5054536-format-xhtml-j9tt2qz/index.html

62 "MP wants IDEMIA banned from doing business in Kenya,"

63 "Nubian Rights Forum & 2 others v Attorney General & 9 others (Interested Parties) [2020] eKLR", last modified May 15, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

64 "Kenya's opposition coalition alleges French OT-Morpho tampered with election results; co. denies allegations," last modified May 12, 2020, https://www.business-humanrights.org/en/kenya-opposition-party-alleges-ot-morpho-complicit-in-tampering-with-election-results-company-denies-allegations

65 "Nubian Rights Forum & 2 others v Attorney General & 9 others (Interested Parties) [2020] eKLR",

66 "MP wants IDEMIA banned from doing business in Kenya,"

67 "Daily Nation, "For credible elections, MPs vote to block Huduma Namba firm, 24 April 2019," last modified 12,2020, https://www.nation.co.ke/news/MPs-vote-block-Huduma-Namba-firm/1056-5086136-i81dnz/;

The Hansard of the National Assembly, 23rd April 2019, http://www.parliament.go.ke/sites/default/files/2019-04/Hansard%20Report%20-%20Tuesday%2C%2023rd%20April%202019%28P%29.pdf

68 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 13, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

69 Ibid

Security measures in place

Cybersecurity experts state that it's usually not a matter of 'if' but rather 'when' you will be hacked.[70] With the ever increasing cybersecurity risks, threats and breaches, every digital system owner is expected to take steps to protect all their digital data and prepare a crisis management plan for potential hacking or breach of private data. These expectations hold even for the Government in relation to the establishment of NIIMS.

The NIIMS database will host all Huduma Namba data centered on the unique identifier approach which gives a 360 degrees overview of a person's identity. This coupled with the linking of personal data to other government agencies provides an attractive target for hacking. If NIIMS were to be successfully hacked, the data breach would have a nationwide effect potentially exposing all the education, financial, biometric, health, financial and social security data of affected individuals. A scandal much more dangerous than the infamous Cambridge Analytica scandal.[71] In the Huduma Namba case, the potential of the data being compromised was also highlighted by one of the expert witnesses.[72] Since the data would be hosted in a centralized database, it gives hackers an incentive to hack into the systems.[73] The expert witnesses noted that hackers tend to compromise systems when the cost of having the data leaked or held in ransom is more than the benefit of safeguarding it.[74]

In this case Kenya may find itself in a situation such as the Wannacry Ransomware attack where the hackers demanded to be paid a ransom in order to release stolen encrypted data.[75]
Bad actors may also access the data and leak information belonging to marginalized groups in society and expose them to the danger of being targeted or having their information used for negative purposes. A risk also arises from weak links in the system as noted in the Aadhaar case, some of the government entities linked to the database did not have proper safety measures creating vulnerabilities in the system.[76]

Section 20 of the Computer Misuse and Cybercrimes Act penalizes unlawful access to protected computer systems. Though important to have, this provision does not as a matter of fact secure NIIMS. It provides a punishment for any indicted offender but is not in itself a preventive information security measure. Similar penal sanctions in India have not deterred multiple data breaches from occurring including breaches by the government.

70 "You are going to be hacked-it's not "If",it's "When"," last modified May 12, 2020, https://dynasis.com/2017/04/going-hacked-not/

71 "Facebook fined for data breaches in Cambridge Analytica scandal," last modified May 13, 2020, https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

72 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 13, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

73 Ibid

74 Ibid

75 " What is WannaCry ransomware, how does it infect,and who was responsible?," last modified May 13, 2020, https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

76 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 13, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

Identity management experts such as Marit Hansen[77] favour a decentralized system over a centralised system. This is because the former is more vulnerable by having a single point of exposure to cyber attacks.[78] However, from NIIMS description as "a single source of personal information of all Kenyan citizens and registered foreigners"[79] it is undoubtedly a centralised system.

NIIMS is designed to use biometrics for authentication. There are several drawbacks to using biometrics as authenticators including the fact that biometrics are immutable.[80] Whereas passwords or access cards can easily be changed if stolen or compromised, a fingerprint, iris and other biometric characteristic is unchangeable. If stolen, wrongfully accessed or replicated, there is nothing the data subject can do to be on the safe side except opting for passwords or security cards or tokens.[81] In a massive breach at the U.S. Office of Personnel Management, hackers reportedly stole 5.6 million individuals' fingerprints.[82] As a result, the affected government employees and contractors cannot be sure that their fingerprint-based authentication will ever be reliable enough.[83] This would be the same fate of any affected Kenyan should there be a data breach of the NIIMS database currently holding data of over 36 million Kenyan citizens and foreigners. [84]

Sharing of data with third parties

NIIMS is an integrated system and there are possibilities that the collected data may be shared by the Government with the private sector for commercial gain. Human Rights Organizations in the Huduma Case argued that IPRS, the current Government 'single source of truth' database was accessible to private companies at a commercial rate.[85]

A similar approach was witnessed in India and has been the subject of lawsuits resulting in the Supreme Court of India restricting private sector services from being linked to Aadhaar enrolment. The Indian Supreme Court deemed "unconstitutional" section 57 of the Aadhaar Act that allowed private players to ask for consumers' personal data. [86] Critics of Aadhaar had alleged that it could potentially open the door to commercial exploitation and even further a surveillance state of sorts, among

77 Marit Hansen, Privacy and Identity Management, IEEE Security & Privacy, March 2008, p.39 https://www.cs.ru.nl/~jhh/pub/secsem/hansen2008privacy-and-idm.pdf

78 "National Digital Identity Programs: What's Next?, Access Now Policy Paper, May 2018, p.34 https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

79 Section 9A(2) (d) of the Statute Law (Miscellaneous Laws Amendments) Act, 2018, http://kenyalaw.org/kl/fileadmin/pdf-downloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf

80 "4 drawbacks of biometric authentication," last modified May 13, 2020, https://www.ifsecglobal.com/cyber-security/4-drawbacks-of-biometric-authentication/

81 Ibid

82 "OPM says 5.6 million stolen in cyberattack, five times as many as previously thought," last modified May 12, 2020 https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?noredirect=on

83 Ibid

84 "36 million people registered for Huduma Namba," last modified May 12, 2020, https://www.the-star.co.ke/news/2019-05-24-36-million-registered-for-huduma-namba/

85 Interior CS sets terms for accessing details on individuals," las modified May 12, 2020, https://www.businessdailyafrica.com/news/Interior-CS-sets-terms-for-accessing-details-on-individuals/539546-3217642-wrk3v0z/index.html

86 "Supreme Court Of India," last modified May 12, 2020, https://main.sci.gov.in/

other things.[87]

Section 9A (2) (g) of the Registration of Persons Act, grants discretionary power to Kenyan government agencies to collate and reproduce data collected. The Act does not provide for circumstances or limitations for sharing personal data. Further, the Act does not limit the right to correct data to data subjects only. Section 9A (2) (i) allows any person or the state in its own motion to correct errors in the registration register. This raises questions about the ability of third parties to alter personal data of the data subject. The RPA is also silent on conditions of access to the database by third parties/private sectors. Access by third parties introduces new avenues for data breaches.

These issues were raised in the huduma case and the court found that the legal framework guiding the operations of NIIMS is inadequate, and poses a risk to the security of data that will be collected in NIIMS. While the Government explained the measures they had put in place to ensure the safety of the data collected by NIIMS and the security of the system, including the encryption of the data and restricted access, the Court found that there was no specific regulatory framework that governed the operations and security of NIIMS and there was no cogent reason provided for this obvious gap. The Court considered it a very serious lapse as all biometric systems, whether centralised or decentralised, and whether using closed or open source technology, required a strong security policy and detailed procedures on its protection and security which comply with international standards. These principles and standards should be provided and actualized in enforceable regulations that will govern the operation of NIIMS.

The Court went even further to hold that there would be no processing of the biometric data and personal data collected for NIIMS in the absence of an appropriate legal framework in which sufficient safeguards were built in to protect fundamental rights.

3.4 Risk to the Rights of Children

NIIMS registration applies to all persons including children from age six. There is a gap on the adequacy of the legal and data protection framework in relation to protecting the biometric data to be collected from children between the age of 6 and under 18. The legal framework pertaining to NIIMS does not have any special conditions or instructions relating to the protection of information relating to children.

87 "Companies can't ask for Aadhaar anymore - or can they?,"Last modified May 12, 2020, ,https://qz.com/india/1402827/supreme-court-verdict-can-companies-ask-for-aadhaar-anymore/

These issues were also raised in the Huduma case and the Court found that there were some gaps in the Data Protection Act. For example the Act does not define the rights of a child in relation to personal data collected with consent of the parent or guardian and how the information is to be handled once the child turns 18 particularly in light of the evolving capacities of children.

The Court also found that the legislative framework for the protection of children's biometric data collected under NIIMS is inadequate, and needs to be specifically provided for. There is a legislative gap due to the absence of regulations that govern how data relating to children is to be collected, processed and stored in NIIMS despite NIIMS being applicable to children. This is a matter of grave concern as information relating to children is sensitive data and must be handled and managed in a manner that protects the best interest of the child in line with Article 53(2) of the Constitution of Kenya.

3.5 Discrimination, Exclusion and Violation of Socio-economic Rights

Enrolment into NIIMS was based on the possession of an ID number for persons above the age of 18 and birth certificate numbers in the case of children. The Huduma Namba is set to be the single identifier for purposes of education, health care provision, social security, issuance of passports and driving licenses, opening bank accounts, registration of mobile subscriber Identity Module (SIM) cards.

3.5.1 Right to Legal Identification

A study by Cenfri indicates that 38 per cent of the Kenyan population does not have a legal means to prove their identity resulting in exclusion.[88] As a percentage, 95.4 percent of individuals without a legal identity are in the lower-income groups compared to 4.6 per cent that are in higher-income groups. The requirement for a national ID as a prerequisite for Huduma Namba registration coupled with the intention to have Huduma Namba as the single pass for life and living in Kenya created circumstances enabling the exclusion of persons without national IDs from accessing Government services such as health. Many Kenyans in towns and villages outside of Nairobi and other major cities lack national IDs, birth notes, birth certificates, alien cards, passports etc. because their local registration centres are far away or they have to wait longer for papers because those centres are overwhelmed.[89]

88 "Cenfri report," last modified May 13, 2020, https://cenfri.org/wp-content/uploads/2018/03/Biometrics-and-financial-inclusion_Cenfri-FSDA_March-2018-2.pdf

89 "Kenya's New Digital IDs May Exclude Millions of Minorities," last modified May 12, 2020, https://www.nytimes.

It has been reported that the Kenyan government has long made it harder, or even impossible for members of some ethnic groups, such as Nubians, Somalis, Maasais, Boranas, Indians and Arabs, to apply for documents required for processing of national ID cards excluding them from the current Registration of Persons Act framework.[90] The affected persons and communities are often asked to present land titles or the papers of their parents and grandparents, in addition to being vetted by security agencies.[91] And often, they can apply for the documents only on specific days of the week [92] or in certain seasons, especially in small towns and rural areas.[93] In Nairobi County for example, the Nubian Community is subjected to a vetting process during national ID registration. Consequently, the community has suffered decades of discrimination in the process of acquiring Identity documents.[94] These additional steps and restrictions are not required for other communities.

Members of some of the affected communities live along Kenya's borders, and government officials say they have introduced the measures to keep out those who pose a security risk, or people fleeing war in neighboring Somalia.[95] However, the measures also affect pastoralists who cross back and forth along the country's borders, such as the Maasai and Samburu.[96]

These hurdles have affected at least five million of Kenya's 47.5 million people, leading to delays in processing their national ID cards and outright denials according to Laura Goodwin, the citizenship program director for Namati, an international legal justice group.[97]

Minority groups such as the Makonde, the Shona as well as pastoral communities[98] and tribes lack conclusive proof of citizenship. If these issues are left unaddressed, those lacking a national ID card will be excluded from enrollment in NIIMS system. [99]Such exclusion would preclude them from access to basic and essential services such as healthcare, education, telecommunications, access to finance, government services and voting. Already a significant number of members of the Nubian community were turned away from NIIMS registration centres for lack of various requirements like the ID card during the NIIMS pilot project.[100]

com/2020/01/28/world/africa/kenya-biometric-id.html

90 Ibid

91 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 13, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

92 Ibid

93 "Kenya's New Digital IDs May Exclude Millions of Minorities," last modified May 12, 2020, https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

94 Report of the Truth, Justice and Reconciliation Commission, Volume IV, para.2.1.2, P.45, http://knchr.org/Portals/0/Reports/TJRC_Volume_4.pdf

95 "Kenya's New Digital IDs May Exclude Millions of Minorities," last modified May 12, 2020, https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

96 Ibid

97 Ibid

98 Ibid

99 "Why some Nubians risk missing out on Huduma Namba," last modified May 13, 2020, https://www.the-star.co.ke/counties/nairobi/2019-05-15-why-some-nubians-risk-missing-out-on-huduma-namba/

100 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 13, 2020, http://kenyalaw.org/case-

Digitizing the current registration of persons regime in the absence of specific, proactive measures to recognize, cater for or even acknowledge persons who lack formal proof of identification will result in further exclusion of these persons and communities.

3.5.2 Political Rights

Article 38 of the Constitution provides for political rights including the freedom of citizens to make political choices and the right to form and participate in political parties, the right to campaign, the right to participate in free, fair and regular elections, the right to be registered as a voter as well as the right to be a candidate for any public office or office within a political party. The requirement for the national ID for voter registration means that 38% (18,074,432) of Kenyans currently not able to prove their legal identity cannot effectively exercise their political rights.[101]

This is quite a significant number of the population particularly in view of the fact that according to the the Independent Electoral and Boundaries Commission (IEBC), there were 19,611,423 registered voters in 2017.[102] The number of persons in Kenya unable to prove their legal identity almost equals the number of registered voters in the last election. The use of Huduma Namba in voter registration has the potential to lock out all persons who are not enrolled in the system from political participation.

Furthermore, the freedom of expression as guaranteed under Article 33 of the Constitution and the right to privacy under Article 31 are closely related to political rights in the absence of express legal and procedural safeguards, a centralized digital ID system such as NIIMS has the potential to be used for targeted surveillance of government dissidents, further curtailing the right to participate in political processes

3.5.3 Access to Government Services

Socio-economic rights are provided for under Article 43 of the Constitution. They include: the right to the highest attainable standard of health, accessible and adequate housing, food of acceptable quality, clean water and social security. Kenya is also a signatory to international treaties such as the International Covenant for Socio-Economic Rights,[103] Universal Declaration of Human Rights[104] and the African Charter and Human and Peoples' Rights.[105] The nexus between legal identity and

law/cases/view/189189/

101 "Kenya census 2019 data reveal population stands at 47.6 million," last modified May 12, 2020, https://www.theeastafrican.co.ke/news/ea/Kenya-population-soars-to-47-million-2019-census/4552908-5336048-7bv3toz/index.html

102 "IEBC certifies final electoral register of 19.6m voters," last modified 12,2020, https://www.nation.co.ke/news/politics/iebc-million-kenyans-are-eligible-to-vote/1064-3990230-eqyihlz/index.html

103 "UN General Assembly, International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, 16 December 1966, A/RES/2200," last modified May12,2020 https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_2200A(XXI)_civil.pdf

104 "UN General Assembly, Universal Declaration of Human Rights, 10th December 1948, 217 A (III)," last modified May 12, 2020, https://www.un.org/en/universal-declaration-human-rights/

105 "Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982)," last modified May 12, 2020, https://www.refworld.org/docid/3ae6b3630.html

access to socio-economic rights cannot be ignored.[106] Governments are increasingly using ICT to implement these rights.

The Kenyan government has made great strides in using Information Communication Technology to improve service delivery.[107] For instance, the e-citizen platform[108] offers almost every government service from applying for a driving licence to formation of companies. Other initiatives include the i-tax platform[109] and the National Health Information System.[110] The latest e-government initiative has been the Huduma Namba, touted as a new era in modern governance.

Section 9A of Statute Law Miscellaneous (Amendment) Act No. 18 of 2018[111] states that data collected under NIIMS is intended to be used across government departments. These include issues of: identification cards, Refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel documentation, student identification, and all forms of government identification including national health insurance and processing of social security benefits.

While the Huduma Namba promises to improve the efficiency of government service delivery, its unintended consequence would be the exclusion of persons not having a Huduma Namba. As already discussed, marginalized and minority groups who already have challenges accessing identification documents will be excluded. The impact of digital identity technologies to include everyone or exclude persons narrows down to its design and implementation. [112]

NIIMS will impact access to mobile telecommunications in Kenya as it is proposed that Huduma Namba will be used in the registration of SIM-cards[113] under the Kenya Information and Communication Act.[114] Consequently, not having a Huduma Namba negatively impacts access to mobile telecommunications, information and financial services.

---

106 Open Society Foundations, " How a Legal Identity Leads to a Better Life," last modified June 28, 2020, https://www.opensocietyfoundations.org/voices/how-legal-identity-leads-better-life

107 "E-Government Strategy: The Strategic Framework, Administrative Structure, Training Requirements and Standardization Framework," last modified May 12, 2020, https://www.ict.go.ke/wp-content/uploads/2019/05/KENYA-E-GOVERNMENT-STRATEGY-2004.pdf

108 " eCitizen website," last modified May 12, 2020, https://www.ecitizen.go.ke/

109 "Kenya Revenue Authority," last modified May 12,2020, https://itax.kra.go.ke/KRA-Portal/

110 " Kenya Health Information System Policy," last modified May 12, 2020, https://extranet.who.int/countryplanningcycles/sites/default/files/country_docs/Kenya/health_information_system_policy.pdf

111 " Statute Law Miscellaneous (Amendment) Act No. 18 of 2018," last modified May 12, 2020, http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf

112 "Digital identity: Contemporary Challenges for Data Protection, Privacy and Non-discrimination Rights," last modified May 12, 2020, https://journals.sagepub.com/doi/pdf/10.1177/2053951719855091

113 "Government to block sim cards whose owners fail to beat Huduma Namba deadline," last modified May 12, 2020, https://www.standardmedia.co.ke/business/article/2001321603/huduma-namba-government-to-block-sim-cards

114 "Government to block sim cards whose owners fail to beat Huduma Namba deadline," last modified May 12, 2020, https://www.standardmedia.co.ke/business/article/2001321603/huduma-namba-government-to-block-sim-cards

Mobile technology has had a positive impact on socio-economic rights in Kenya. For instance in 2018, mobile money transactions contributed $144.1 billion economic value which translates to 8.6% of the region's GDP.[115] In Kenya, the Eneza [116]Platform provides revision and learning material via basic feature phones while M-Pesa is a mobile banking service which allows ordinary Kenyans to access financial services such as mobile banking, payments, and loans.[117] Essentially, not having a Huduma Namba will be a determinant factor in enjoying socio-economic rights on mobile phones.

Many Government services are currently predicated on the possession of an ID card. In Kenya, you need an ID to register for Government benefits and to access Government buildings.[118] The ID is required for registration for medical health insurance, social security, employment, property transactions, mobile money registration and bank account opening amongst other services. Once NIIMS is fully implemented, Huduma Namba will be a prerequisite for access to these services.

The Cenfri study report indicates that 19 percent of the Kenyan adults cite the lack of a formal identification document as the reason for not having a bank account. In Uganda, Tanzania, Rwanda, and Ethiopia, the rate is at 24 percent, 27 percent, 8 percent, and 2 percent respectively. The lack of a formal identification results in people moving to the informal sector and eventually lead to illicit activities. The report also notes that the greatest challenge to financial inclusion is the lack of reliable identification mechanisms and verification for individuals.[119]

Further, the 38% of Kenyans unable to prove their legal identity run the risk of being denied key government services such as healthcare, education, fertilizer subsidies, cash transfer and affordable housing. Under NIIMS, everyone is reduced to a digital identity without which government and other key services cannot be accessed. As per Huduma Case, members of the Nubian Community have missed employment opportunities due to lack of proof of Kenyan citizenship or work permits. This has largely interfered with their ability to earn income and hold property as without an ID, one cannot register for a KRA PIN certificate required for property transactions.

Further, NIIMS relies on biometrics and therefore persons with biometric features which make it challenging or impossible to authenticate are also likely to be excluded, for example, labourers whose fingerprints wear out in time. There is a need to develop backups and redundancy features that ensure one is not locked out of NIIMS for factors which are beyond their control.

---

115 "The Mobile Economy in Sub-Saharan Africa 2019," last modified May 12, 2020, https://www.gsma.com/mobileeconomy/wpcontent/uploads/2020/03/GSMA_MobileEconomy2020_SSA_Eng.pdf

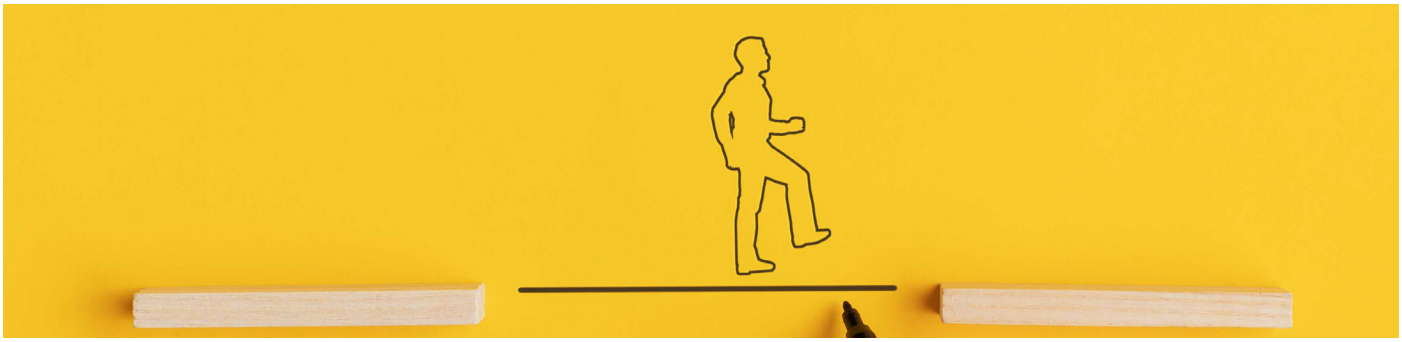
116 "Eneza Education:Home," last modified May 13, 2020, https://enezaeducation.com/

117 "M-Pesa website," last modified May 12, 2020, https://www.safaricom.co.ke/personal/m-pesa

118 "Study on the Issuance of National Identity Cards In Kenya," last modified May 12, 2020, https://www.knchr.org/Portals/0/EcosocReports/KNCHR%20Final%20IDs%20Report.pdf

119 "Centri report," last modified May 12, 2020, https://cenfri.org/wp-content/uploads/2018/03/Biometrics-and-financial-inclusion_Cenfri-FSDA_March-2018-2.pdf

The above issues were raised in the Huduma Case and the Court found that while there was no evidence on record suggesting that using NIIMS would be discriminatory to the Nubian People, there are still gaps in the current legal framework creating a risk that a segment of the population may be excluded from government recognition if NIIMS is implemented under the current legal framework.[120] The Court stated that the Government needs to provide a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework needs to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS.[121] The possibility of this exclusion is in itself not a sufficient reason to find NIIMS unconstitutional or in violation of the right to non-discrimination or equality before the law.[122]



3.6 Gaps in New Regulations

Following the judgement issued in the *Huduma Namba* Case, the government developed and published two sets of draft regulations: *The Registration of Persons (National Integrated Information System Regulations 2020* [123] and *the Data Protection (Civil Registration) Regulations, 2020.*[124] These aim to provide the required enabling legal framework for continued roll out of NIIMS. These draft regulations have been presented to the public for review and input.

3.6.1 The Registration of Persons (National Integrated Information System Regulations 2020

The Registration of Persons (National Integrated Information Management System) Regulations, 2020 is made under the Registration of Persons Act. It provides for definition of terms related to NIIMS; the structure, components and functions of NIIMS, the Huduma Database, Huduma Card and Huduma Numba; the enrollment of minors, adults and foreign nationals to NIIMS; the issuance of Huduma Namba and Huduma Card; procedure for updating information on NIIMS; the application of the

120 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 13, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

121 Ibid

122 Ibid

123 "The Registration of Persons (National Integrated Identity Management System) Regulations 2020," last modified May, 13 2020, https://ict.go.ke/wp-content/uploads/2020/02/THE-REGISTRATION-OF-PERSONS-NATIONAL-INTEGRATED-IDENTITY-MANAGEMENT-SYSTEM-REGULATIONS-2020.pdf

124 "The Data Protection (Civil Registration) Regulations, 2020," https://ict.go.ke/wp-content/uploads/2020/02/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-2020.pdf

Data Protection Act to NIIMS as well as the access of NIIMS by various Agencies (other than Ministry of Interior).

The key legal gaps present in these draft regulations are discussed below:

Inadequate definition of terms: it is not clear what the word 'Agency' means when referencing parties that may access NIIMS.[125] It is not apparent whether it refers to both private and public agencies or just Government Agencies. They also fail to elaborate whether private entities access the database or stipulate the procedures for requesting access as well as the terms of access including any relevant charges. It does not also include minimum data protection and cybersecurity thresholds. As the draft Bill stands, access by private entities presents potential data infringement and cybersecurity risks.

Exclusion concerns: The regulation does not have clear and express provisions addressing the possibility of exclusion from registration to NIIMS, or regulating the manner in which those without access to identity documents, or with poor biometrics will be enrolled in NIIMS/access Government services they are entitled to. The absence of such critical provisions may create barriers to access government services for those who do not have a Huduma Namba. The absence of such provisions may even occasion death where one is denied access to medical services including emergency care for lack of Huduma Namba registration or for failure of biometric authentication.

Lack of clarity on the retention or transition of registration of persons' regimes: The government has not stated whether the current legal framework for registration of persons (under the various registration laws) will still hold, and if not what amendments would need to be made to changes to various Acts including the Registration of Person Act, the Kenya Citizenship and Immigration Act and the Registration of Births and Death to reflect the use of NIIMS. It must be noted that this can only be done via an Act of Parliament and not Regulations.

The lack of clarity on the process of enrollment and the documents that are required: The regulations do not specify the mandatory documents required for enrollment. It also does not provide including any prescribed enrollment forms to be filled.

Lack of express purpose limitation provisions for use of data by Government agencies: The regulation lacks clarity or express provisions on purpose or use of data by different Government agencies. It also lacks procedures for access and safeguards against abuse by any corrupt officials. Further, it does not provide for any special penalties for misuse or abuse of information by Government or private entity officers

125 "The Draft Registration of Persons (NIIMS) Regulations 2020," last modified May 12, 2020, https://blog.cipit.org/2020/03/19/the-draft-registration-of-persons-niims-regulations-2020/

3.6.2 Data Protection (Civil Registration) Regulations, 2020

The draft *Data Protection (Civil Registration) Regulations, 2020*[126] was formulated by the Cabinet Secretary for ICT under section 71 of the Data Protection Act 2019. It expounds on the rights of the data subject in relation to civil registration. The regulations provide for the data protection principles applicable to NIIMS database, the rights of the data subject, obligations of the civil entities collecting this data,[127] the security safeguards required to ensure that personal data is adequately protected, the criteria for conducting a data impact assessment, as well as the prescribed forms for requesting the deletion of data or restriction of processing of personal data.[128] If adopted, the draft regulations would bring NIIMs under the purview of the Data Protection Act.

While section 51 of the data protection Act exempts NIIMS from its scope, these regulations offer a parallel data protection regime for data collected under NIIMS. We note that some of the Regulations are similar to the Data Protection Act provisions namely; section 24(7) on the duties of a Data Protection Officer under regulation 20, section 31 on data protection impact assessment under regulation 19 and section 43 on notification of breach is reflected in regulation 18.

Notable divergence from the Act include regulation 17 which states that data collected during civil registration will be retained in perpetuity while section 39 of the Act limits data retention only for as long as is necessary after which the data should be deleted, erased or pseudonymised. Additionally regulation 21 sets out grounds for sharing personal data with other public agencies while section 25 has the right to privacy as its core value.

Other key legal gaps relating to these regulations are discussed below.

Non-compliance with procedure for the promulgation of regulations: The regulation has been drafted before the establishment of the Office of the Data Commissioner under the Data Protection Act. Under section 71 of the Act, regulations should be formulated by the Data Commissioner in consultation with the Cabinet Secretary for ICT. Due process has not been followed as the regulations have been drafted in the absence of the establishment of the Office of the Data Protection Commissioner.

Exclusion of some registries from definition of Civil registries: the regulations are very specific on what constitutes a civil registry. The definition does not include some existing entities that collect personal data such as the Kenya Revenue Authority, National Hospital Insurance Fund and the National Social Security Fund registries.[129]

Lack of clarity on retention or transition from IPRS: The regulations do not address the retention of the IPRS database or in the alternate, the transition from IPRS to NIIMS and specifically what will happen to IPRS data once NIIMS is established.[130]

126 Ibid

127 Ibid

128 "KICTANET online conversations on the Regulations," last modified May 12, 2020,

129 Data Protection (Civil Registration) Regulations, 2020,"

130 "KICTANET online conversations on the Regulations,"

Silence on access of data by private sector entities: The regulations do not permit or ban access of the NIIMS database by private entities. It does not specify whether private entities will be allowed to access the database and if so on what terms and conditions. There are no provisions for minimum security safeguards, data protection requirements, duration of access, purpose of access, consent of the data subject and charges if any.

Implementation challenges: There could be challenges in the adoption and implementation of the regulation as the office of the Data Protection Commission is yet to be established.[131]

Consent for information collected in childhood: The regulations are not clear on whether minors, upon attaining age of majority, can revoke any consent their parents gave on their behalf regarding the collection and use of their data.[132]

Bias due to automatic decision making: The regulation envision the use of automated systems in decision making processes. Depending on the data fed to this system as well as the predispositions of the designers and coders, bias may arise. This is not adequately addressed and neither are measures or principles provided to identify and minimise the impact of bias in automated decision making.

Charges for data portability requests: The regulations provide in clause 13 that data portability requests shall be honoured after payment of the prescribed fee. The fee is not stated.

Frequency of compliance reports from external service providers: Clause 40 provides that external service providers should file compliance reports with the civil registry annually. 39 provides that civil registries file compliance reports with the Office of the Data Commissioner every quarter. Regulation 40 should be reviewed to require external service providers to file reports every quarter.

3.7 High Cost of Implementation

The cost of implementing the Huduma Namba project raises another problem that may lead to lack of proper deployment. When the Huduma Namba project was first commissioned, the government budgeted for about. 7 billion[133] to conduct the mass registration exercise, which later increased to Kenya Shillings 7.7 billion.[134] It is estimated that the government eventually spent Kenya Shillings 9.6 billion yet the project remains incomplete.[135]

131 "Submissions on the Data Protection Civil Registration Regulation (2020) in Kenya," last modified May 13, 2020, https://openinstitute.com/data-regulations/

132 Ibid

133 Sh 1bn budget cut delays huduma namba cards, https://www.businessdailyafrica.com/news/Sh1bn-budget-cut-delays-Huduma-Namba-cards/539546-5357946-u6jk63z/index.html

134 "Huduma Namba Frequently Asked Questions," last modified May 12, 2020, http://www.hudumanamba.go.ke/faqs/

135 "Lower Budget Signal Huduma Cards Scaledown," last modified May 12, 2020, https://www.businessdailyafrica.com/economy/Low-budget-signals-Huduma-cards-scaledown/3946234-5551800-6p4cmx/index.html

Financial challenges in implementing NIIMS were first witnessed when the government delayed paying the staff hired to assist in the mass registration 6 months after the first phase mass registration was completed.[136] Moreover, the Government was preparing to begin roll out of the Huduma Card, the National Treasury slashed the budget by 1 billion Kenya Shillings under the supplementary budget 2019/2020.[137]

Further, in the new budget estimates for the year 2020/2021 the government has only allocated 500 million Kenya Shillings to the printing of the Huduma cards.[138] Should printing begin, the allocated budget would only be able to print cards for half of the enrolled population.[139]

As of 26th May 2020, the Government proposed to assign Kenya shillings 2.05 billion to Huduma Namba roll out for the financial year 2021/2022. However, this proposed allocation is not assured. [140]

Further, the National Assembly under the financial year 2019/2020 had requested the Office of Auditor General carry out a special forensic audit of the National Integrated Identity Management Systems (NIIMS) to establish the value for money and submit a report to the National Assembly by end of March 2020. This had not complied with due to the lack of a substansive holder of office and delays in recruitment,[141] A substantive Auditor General was sworn into office in July 2020.[142]

Over the past few years and increasingly since COVID-19 pandemic was announced, revenue collection in Kenya has witnessed a downward trend. The government finds itself in some financial difficulty with regard to availing resources for complete roll out of Huduma Namba and issuance of huduma cards. Under such circumstances, there is a risk that the Government may easily overlook crucial infrastructure and adherence to policy and procedures relating to safeguards required for NIIMS under the guise of cost cutting measures. Further, the government may lack adequate resources to employ required and qualified manpower to monitor and maintain the NIIMS system.

---

136 "Questions for Matiang'i over Huduma Namba," last modified May 12, 2020, https://www.standardmedia.co.ke/article/2001350698/questions-for-matiang-i-over-huduma-namba

137 "2019/20 Supplementary Estimates 1 for the Year Ending 30th June 2020 pg.35," last modified May 12, 2020 https://www.treasury.go.ke/component/jdownloads/send/209-supplementary-budget-books/1559-pbb-supp1-draftbook-3-2019.html "Sh. 1bn bidget cuts delays Huduma Namba Cards," last modified May 12, 2020, https://www.businessdailyafrica.com/news/Sh1bn-budget-cut-delays-Huduma-Namba-cards/539546-5357946-u6jk63z/index.html

138 "2020/2021 Supplementary Estimates 1 for the Year Ending 30th June 2021 pg.49," last modified May 12, 2020 https://www.treasury.go.ke/component/jdownloads/send/216-budget-books/1566-pbb-2020-21-draft-28-04-2020.html "Low Budget Signals Huduma Cards Scaledown," last modified May 12, 2020, https://www.businessdailyafrica.com/economy/Low-budget-signals-Huduma-cards-scaledown/3946234-5551800-6p4cmx/index.html

139 "2020/2021 Supplementary Estimates 1 for the Year Ending 30th June 2021 pg.49," last modified May 12, 2020 https://www.treasury.go.ke/component/jdownloads/send/216-budget-books/1566-pbb-2020-21-draft-28-04-2020.html

140 Ibid

141 Parliamentary Budget Office, "Unpacking the Estimates of Revenue and Expenditure for 2020/2021 and the Medium Term," http://parliament.go.ke/sites/default/files/2020-05/unpacking%20of%20the%202020%20budget%20final%20word_0.pdf

142 Gathungu sworn in as new Auditor General https://www.standardmedia.co.ke/nairobi/article/2001379092/gathungu-sworn-in-as-new-auditor-general

Were these risks to materialize, data on NIIMS would be compromised due to lack of adequate budgets or measures to ensure the data is managed in keeping with the Data Protection Act.

This section reviews the emerging best practice with respect to digital identity systems including some digital identity initiatives in countries such as Estonia, India, and the United States.

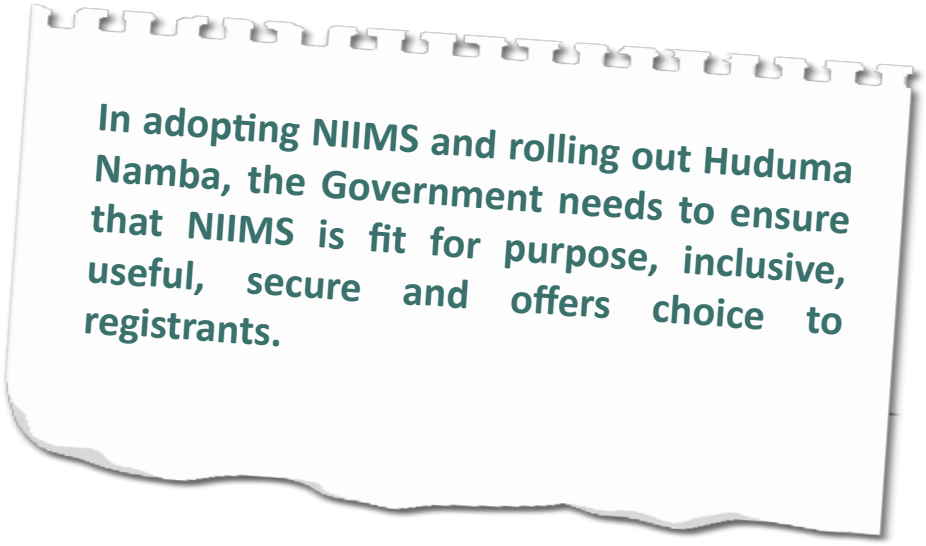
Emerging Best Practises

4.0

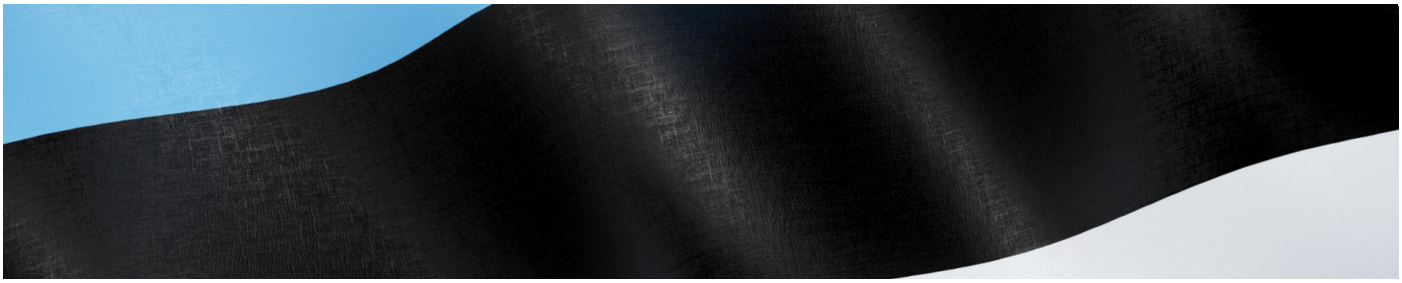
4.1 Global Initiatives

At the World Economic Forum's Annual Meeting 2018 in Davos, a diverse group of public and private stakeholders committed to shared cooperation on advancing good, user-centric digital identities. Consequently, the Forum in its 2018 Insight Report, outlines key aspects that a good Digital Identity System should have, which include:[143]

1. **Fit for purpose:** Good digital identities offer a reliable way for individuals to build trust in who they claim to be, to exercise their rights and freedoms, and/or demonstrate their eligibility to access services.
2. **Inclusive:** For inclusive identity there should be nostructural barriers that prevent anyone from accessing the systems and the registration/identity system should enable anyone to access it without risk of discrimination.
3. **Useful:** Useful digital identities offer access to a wide range of useful services. Further, the law should provide the specific uses of the Data collected and the consequences of using the data for other purposes rather than the ones stated in the law.
4. **Offers choice:** Individuals should be given a choice as to how their data is used, who has access to the data and how long the data is stored. Individuals should not be denied access to basic services such as health care due to lack of a digital identity.
5. **Secure:** There should be proper technical measures in place as well as from identity theft, unauthorized data sharing and human rights violations. The laws should also restrict lawful interception and monitoring of digital identities as this may lead to the monitoring and privacy invasion of people regarded as unfriendly to the government.



143 "Identity in a Digital World," last modified May 13, 2020, http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf



4.2 Estonia

Estonia has one of the most advanced digital identity systems in the world.[144] The Digital ID has multiple uses and is a legal document used as a legal travel ID for Estonian citizens travelling within the European Union (EU), a national health insurance card, proof of identification when logging into bank accounts, for digital signatures, for I-Voting, to check medical records, to submit tax claims, e-Prescriptions and as a digital signatures.[145] This is ideally the Kenyan Government's vision for *Huduma Namba.*

One can apply for the Estonian ID if they are citizens of Estonia or legal Aliens. The cards are renewable every five years.[146] The user is able to monitor any activities in relation to the use of their card.[147]

Estonia encountered some challenges while implementing their digital ID system including how to effectively and securely identify residents using public and private e-services. This challenge was magnified in April 2007 when Estonia was hit by the largest organized cyber-attack against a single country.[148] In response,the Estonian government and cryptographers developed a KSI blockchain system that is now used by government agencies to back up their data.[149] KSI is a blockchain system that was created by the Estonian government to make sure networks, systems and data are free of compromise, all while retaining 100% data privacy.[150] It is encrypted to back various government registries and it has proved to be an effective tool in safeguarding the peoples Data. [151]

The Estonian government put in place a proper legal framework to ensure that the citizens data was adequately protected. In addition, it was transparent on how the data was used and stored.[152] Further, through the various government portals it provides adequate information on digital identity. For example, one can view the Active ID-cards, Active Mobil-ID, Active Smart-ID, Active Smart-ID in Estonia, transactions from the previous day that used the digital ID and transactions from the previous month on the online portal.[153]

144 ID-card-e-Estonia," last modified May 13, 2020 https://e-estonia.com/solutions/e-identity/id-card/

145 "ID-card-e-Estonia," last modified May 13, 2020 https://e-estonia.com/solutions/e-identity/id-card/

146 Ibid

147 Ibid

148 "e-Estonia;We have built a digital society and we can show you how," last modified May 13, 2020, https://e-estonia.com/#-timeline

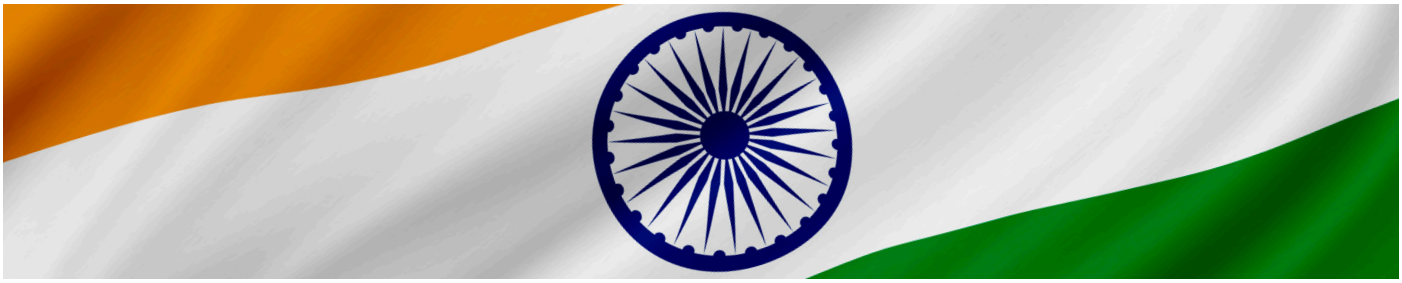
149 Ibid

150 "KSI Blockchain e -Estonia," last modified May 14, 2020, https://e-estonia.com/solutions/security-and-safety/ksi-block-chain/

151 "e-Estonia;We have built a digital society and we can show you how," last modified May 13, 2020, https://e-estonia.com/#-timeline

152 "e-Estonia;We have built a digital society and we can show you how,"

153 "Home > ID.ee," last modified May 13, 2020, https://www.id.ee/?lang=en&id



4.3 India

In 2011, India initiated a new digital identity document known as the Aadhaar Card and established a new agency, the Unique Identification Authority of India (UIDAI), to issue the card.[154] Aadhaar has a twelve digit unique identity number. The government intended for Aadhaar to be the primary identity number for all legal Indian residents.[155] It also made Aadhaar available to every legal resident free of cost. In order to apply for the card, a resident is required to submit their biometric data, which includes a scan of their fingerprints and retinas and a passport photo.[156] The UIDAI is responsible for storing the data in a centralized database.

According to the government Aadhaar is devoid of any intelligence and does not profile people on any ground.[157] The Aadhaar database runs on an open source software platform thus precluding the use of dependence on one specific hardware, storage, specific OS, specific database vendor, or any specific vendor technologies to scale.[158] The Indian government progressively made the Aadhaar card mandatory for numerous welfare schemes. These include subsidized food under the Public Distribution System and the Mid-Day Meal Scheme and guaranteed wage labour under the Mahatma Gandhi National Rural Employment Guarantee Scheme.

Several challenges have arisen from the Aadhaar system including:

- **Data breaches:** Aadhaar is not completely secure and data from the system has been occasionally compromised.[159] Due to the fact that the system is connected to other private entity systems which have potential weaknesses in their systems, hackers can easily use those vulnerabilities to access data on Aadhaar.[160]

- **Discrimination:** Initially the government had made it a compulsory requirement to have an Aadhaar number in order to access government services, to register a bank account or a sim card and to enroll into a learning institution.[161]

---

154 "Constitutionality of Aadhaar Act," last modified May 13, 2020, https://www.scobserver.in/court-case/constitutionality-of-aadhaar-act

155 Ibid

156 " What is Aadhaar," last modified May 13, 2020, https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html

157 Ibid

158 "Features of Aadhaar," last modified May 13, 2020, https://uidai.gov.in/my-aadhaar/about-your-aadhaar/features-of-aadhaar.html

159 "Aadhaar Verdict: Why Privacy still Remains a Central Challenge," last modified May 14, 2020, https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms?from=mdr

160 Ibid

161 "Everything You Need to Know about the Aadhaar Verdict," last modified May 14, 2020, https://economictimes.indiatimes.com/news/politics-and-nation/whats-valid-and-whats-not-everything-you-need-to-know-about-todays-aadhaar-verdict/articleshow/65961427.cms?from=mdr

- **Duplicity of registration:** During initial roll-out, there was an assumption that Aadhaar would be 100 % percent duplication proof. This has proved false.[162]

- **Inflated enrollments:** After the initial enrollment, the government of India eventually found that some of the Aadhaar data was inflated because the data collectors were paid by the number of persons enrolled. Some registration clerks exaggerated the number of enrollments done in order to get paid more money.[163]

- **Surveillance Issues:** The authentication mechanism under Aadhaar system leads to the creation of authentication logs.[164] Each time Aadhaar is used to authenticate one's identity, the log notes metadata of such authentication.[165] Experts have noted that when done at scale and over a long period of time, such authentication logs can be a tool for pervasive profiling and surveillance.[166]

The Aadhaar scheme was challenged before the Supreme Court of India by Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court. He claimed that Aadhaar infringed upon fundamental rights guaranteed by the Constitution. Broadly, his objections included assertions that:

- The government had not put in place adequate privacy safeguards;

- Any private entity was allowed to request authentication by Aadhaar for any reason subject to regulations by the UIDAI;

- There were no checks on the power of the government to use the biometric data collected; and,

- Entitlements granted to the individuals by the State's social sector schemes were themselves a fundamental right and could not be limited for any reason, including the failure to produce an Aadhaar Card or Number when applying for benefits.

On 26th September 2018, the Supreme Court of India delivered its judgment upholding the Aadhaar Act as constitutionally valid. It ruled that the Act empowered disenfranchised sections of society by providing them better access to fundamental entitlements, such as State subsidies. The Court held that the Act was competently passed by Parliament and thus did not violate the fundamental rights guaranteed under Articles 14, 15, 19 and 21 of the Indian Constitution. The court however ruled that:

- Section 57 of the Aadhaar Act was unconstitutional. Consequently, no company or private entity is entitled to seek Aadhaar identification from an Indian resident. Private companies including banks, e-wallets, and telecommunication service providers should not ask for Aadhaar to give services.

---

162 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 14, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

163 Ibid

164 "National Digital Identity Programmes: What's next? Access Now Policy Paper 2018," last Modified August 22, 2020, https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

165 Ibid

166 Ibid

- Aadhaar number is not compulsory for school admission;
- Illegal immigrants should not be given Aadhaar numbers;[167]
- Aadhaar is mandatory for filing of income tax returns (ITR) and allotment of Permanent Account Number (PAN) as well as for availing facilities of welfare schemes and government subsidies to empower the poor and marginalised;
- No child should be denied benefits of any scheme if he or she doesn't have an Aadhaar card;
- Aadhaar would not lead to a surveillance state because the data was kept in silos. The program's invasion of privacy was minimal and served a much larger public interest by providing identities to India's poor and marginalized citizens; and,
- Difficult to profile a person on the basis of the minimal biometric information collected.

India has experienced a number of data breaches on its Aadhaar System. For example hackers were found to have created 26 patches to the Aadhaar enrolment software. [168] These patches allowed the Global Positioning System (GPS) tracking the device's location to be disabled bypassing the need to authenticate the enrolment operators by running the image file of the operator's biometric.[169] In effect, an Aadhaar enrolment station could be set up anywhere in the world. The original intent of the software was to have the device GPS-locked, so that no one could operate an enrollment centre outside India.[170] However, with the data obtained by the hackers they could create logins from anywhere in the world and enable people who are not Indian citizens to log into Aadhaar.

167 "Justice K.S. Puttaswamy (Retd.) and Another v Union of India and Others," last modified May 14, 2020, https://sflc.in/updates-aadhaar-final-hearing/aadhaar-judgement

168 "Aadhaar verdict: Why privacy still remains a central challenge," last modified May 12, 2020, https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms?from=mdr

169 Ibid

170 "Aadhaar Verdict: Why Privacy still Remains a Central Challenge," last modified May 13, 2020, https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-why-privacy-still-remains-a-central-challenge/articleshow/65970934.cms?from=mdr

4.4 United States of America

In the United States, a Social Security Number (SSN) is a nine digit number that enables persons in the US to access social security services.[171] The Social Security Number is however not a Digital Identity Number. The purpose of the number is to enable the US government to identify and accurately record an individual's wages or self-employment earnings, and to monitor an individual's record once they start getting benefits.[172]
When Social Security Numbers were introduced in the USA their sole purpose as described was for tracking a worker's lifetime earnings in order to calculate retirement benefits after age 65.[173] Up until 1972 the cards stated that they are not a form of Identification Number and only for social security purposes.[174] Only a very narrow set of government agencies and financial organizations are required to ask for a customer's SSN by law.[175] However, due to the lack of a proper legal identification number in the US, private entities and government agencies that are not required by law to request for social security numbers such as credit reporting agencies, landlords and cable companies slowly started relying on it as an identification number even though it was not designed to be one.[176]

Americans are only required to give out their SSN details when becoming an employee or independent contractor for a business, engaging in a banking, financial or real estate transaction, applying for group health insurance through an employer, or when applying for credit. In practice however, even when there is no law requiring it, a business might request one to avail their SSN and deny someone services if they refuse to provide it.[177]

The biggest challenge the US has had in terms of social security number administration, is the number of data breaches that have occurred in relation to SSNs exposing the number owners to identity theft.[178] In February 2020, the Department of Defense Information Systems Agency, which is responsible for providing IT support to combat missions, in addition to securing White House communications, was hacked and Social

171 " Social security Number and Card," last modified May 14, 2020 https://www.ssa.gov/ssnumber/

172 Ibid

173 "Identity crisis: how Social Security numbers became our insecure national ID," last modified May 14, 2020, https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic

174 "Why are we still using Social Security numbers as ID?," last modified May 14, 2020, https://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html

175 "Identity crisis: how Social Security numbers became our insecure national ID," last modified May 14, 2020, https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic

176 Ibid

177 "When am I required to provide my Social Security number to a business?," last modified May 14, 2020, https://privacyrights.org/resources/when-am-i-required-provide-my-social-security-number-business

178 "Identity crisis: how Social Security numbers became our insecure national ID," last modified May 14, 2020, https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic

Security Numbers of its employees stolen.[179] In another instance Equifax, a credit reporting agency was hacked in 2017 leading to almost half of the US population's SSNs being leaked. [180]

Due to the number of data breaches that have happened in the US, companies and entities are slowly starting to realize that the numbers are not enough proof of identification. Even though biometric systems have been suggested as proof of identification, there are concerns that if biometric data is exposed ,one cannot have their biometrics such as fingerprints and iris scans replaced.[181] The risk of permanent damage from identity theft and compromise is higher with biometric based systems as opposed to ID card or number based systems.[182]

The US government has realized the importance and urgency of dealing with SSN and the identity thefts that have occurred due to data breaches.[183] The Social Security department has guidelines that one should follow when they discover that their social security number is being used fraudulently this includes making a report to the Federal Trade Commission via phone or the IdentifyTheft.gov portal.[184] The affected data subject may also report SSN theft to the Internal Revenue Service.[185] A report may also be made to the Internet Crime Complaint Center. The Internet Crime Complaint Center gives victims of cybercrime a convenient reporting mechanism that alerts authorities of suspected criminal or civil violations.[186] It sends every complaint to one or more law enforcement or regulatory agencies with jurisdiction to handle the matter.[187]

The US Government has started discouraging both public and private entities from reliance on the SSN as the single source of truth for one's identification.[188] In 2007, the office of Management and Budget issued guidance requesting the various government agencies to come up with other ways of identifying individuals.[189] However, government agencies are yet to develop alternative identification systems with only the Centers for Medicare and Medicaid Services being coming up with an alternative to the SSN known as Medicare Beneficiary Identifier.[190] USA legislators have argued that the solution is not creating more number based identifiers, but creating a secure tokenized system like the one created by Estonia.

---

179 "Social Security numbers stolen in defense agency data breach," last modified May 14, 2020, https://www.cnet.com/news/data-breach-hits-us-defense-agency-responsible-for-securing-combat-it/

180 "143 million compromised Social Security numbers: everything you need to know about the Equifax hack," last modified May 12, 2020, https://www.theverge.com/2017/9/22/16345580/equifax-data-breach-credit-identity-theft-updates

181 "Why are we still using Social Security numbers as ID?" last modified May 14, 2020, https://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html

182 Ibid

183 "Identity Theft and Your Social Security Number," last modified May 14, 2020, https://www.ssa.gov/pubs/EN-05-10064.pdf

184 Ibid

185 Ibid

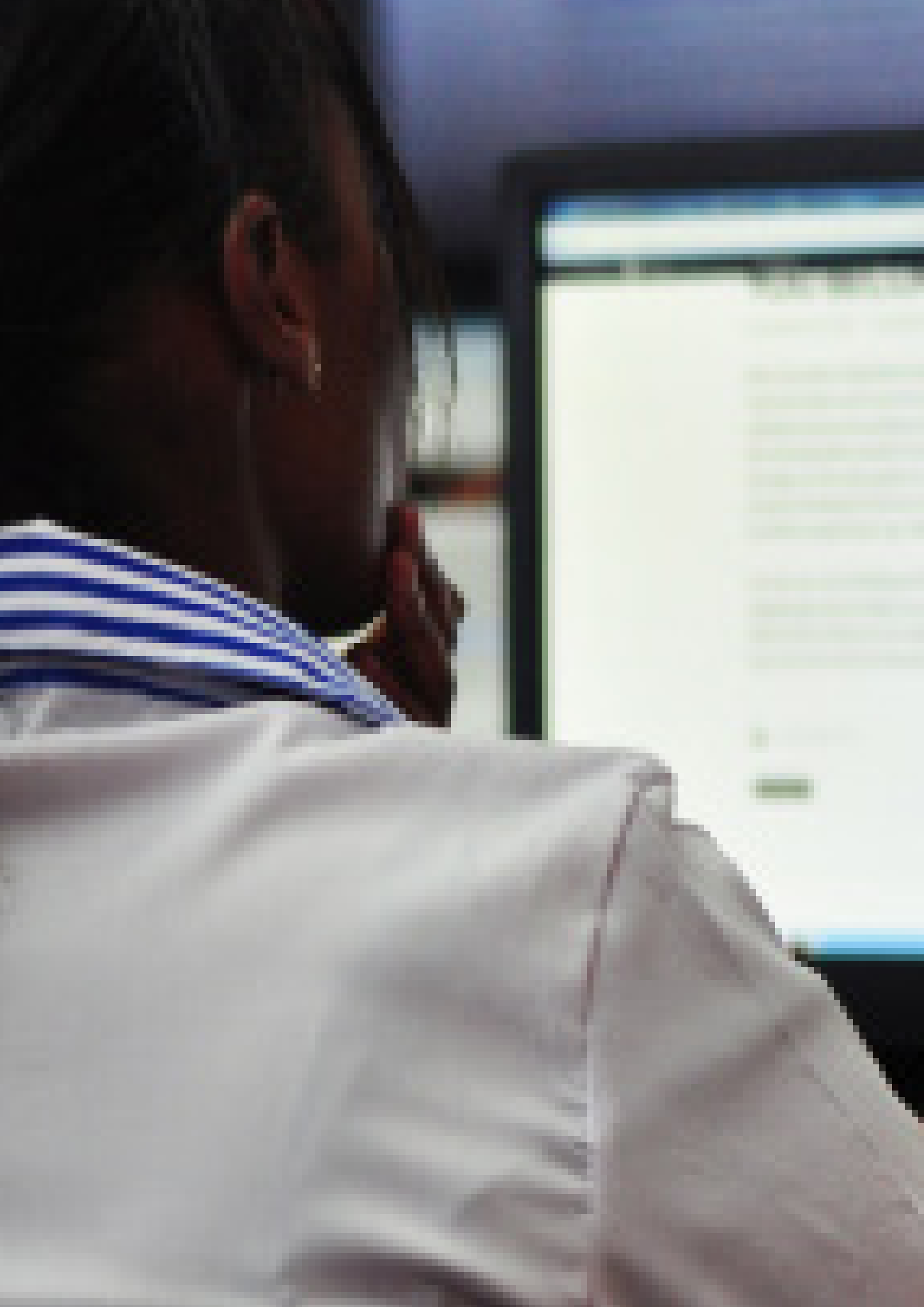
186 Ibid

187 "Identity Theft and Your Social Security Number," last modified May 14, 2020, https://www.ssa.gov/pubs/EN-05-10064.pdf

188 "Social Security numbers: a security risk with serious staying power," last modified May 14, 2020, https://gcn.com/articles/2017/05/30/social-security-numbers.aspx

189 Ibid

190 Ibid



Conclusion & Recommendations 5.0

5.1 Conclusions

The Huduma Namba initiative is commendable given its objective to provide digital identity to residents of Kenya. It is a step in the right direction and fits within the broader international framework for provision of legal identities.

5.2 Recommendations

There are various actors involved in the Kenya Huduma Namba Project who are key stakeholders influencing successful implementation of NIIMS. This segment presents study recommendations relevant to various key stakeholders.

5.2.1 Government

There are various legal, regulatory and policy interventions required to support implementation of NIIMS in a manner that preserves and provides for human rights in keeping with current local and international norms to which Kenya is bound.

a) Adhere to the constitution in the implementation of Huduma Namba

The government should ensure it is implemented in line with the Constitution of Kenya, the Bill of Rights, in a free and fair manner with due regard for special and vulnerable groups and respecting the principles of governance under Article 10. In particular, it should involve all stakeholders in the implementation process, implement court orders as given in the Huduma Namba case, and, spearhead the formulation of laws, policies and regulations that fill the legal gaps identified in order to ensure implementation of NIIMS does not negatively affect human rights guaranteed under both national and international law.

Further, Parliament needs to lead in providing a definition or parameters for what amounts to sufficient public participation. This needs to be addressed, particularly in relation to the use of omnibus Bills to make amendments that substantially affect one or more human rights.

b) Ensure a Strong Data Protection Framework

The government should develop, adopt and champion regulations to give effect to the Data Protection Act. In particular, the regulations should outline circumstances where the Data Commissioner may exempt persons from the application of the Act; provide data sharing codes for the exchange of personal data between government departments; provide circumstances, conditions and limits for the sharing of personal data with third parties or for third party access to databases containing personal data held by government agencies with third parties;elaborate and delimit the right to correct data and clarify persons with authority to rectify data as provided under section 9A (2) (i) of the RPA which allows "any" person or the state on its own motion to correct errors in the registration register, in order to prevent third parties from altering personal data of the data subject. Further, for a digital identity to be empowering, frameworks must be built in a manner that is user-centric and enshrines transparency.[191]

191 "National Digital Identity Programmes: What's next? Access Now Policy Paper 2018," last Modified August 22, 2020,

c) Strengthen Information and System Security

The government should draft, champion and pass regulations for operationalization of the Data Protection Act and particularly regulations:
That provides a specific regulatory framework that governs the operations and security of NIIMS. These can be fashioned like the Indian Aadhaar (Data Security) Regulations, 2016 and the Aadhaar (Sharing of Information) Regulations, 2016, the Aadhaar (Enrolment and Update) Regulations, 2016, The Aadhaar (Authentication) Regulations, 2016.

- Require a strong security policy and detailed procedures on system protection and security which comply with international standards. These principles and standards should be provided and in enforceable regulations that will govern the operation of NIIMS.

- That outlines the technical infrastructure of NIIMS and how each of the parts regarding NIIMS will be designed and maintained. These include the login process, the data storage process, which government agencies will be linked to NIIMS and the safeguards they must adhere to, the redundancy measures in place in case one system fails, what level of access do the people who are accessing the documents have and the measures taken to prevent identity theft or the sale of this data by the officials who have access to it.

- Require the use of cryptography and blockchain to securely implement Huduma Namba should be considered by the Government of Kenya in keeping with sampled case studies and best practice.

d) Prevent Identity Duplication

The Government should:

- Take practical and technical measures to avoid the continuation of identity duplication under NIIMS especially if the government is to rely on the Huduma Namba as the single source of truth for people's identity.

- Provide mechanisms that enable access to basic services such as health care, health insurance and social security benefits for anyone affected by duplication issues under NIIMS as well as administrative procedures with timelines to address any duplication concerns raised or discovered.

- Enact Regulations similar to the Indian Aadhaar Act, the Aadhaar (Enrolment and Update) Regulations, 2016 and the Aadhaar (Authentication) Regulations, 2016.

e) Protect the Best interest of the child

The Government needs to draft, champion and adopt a legal framework with special conditions or instructions relating to the protection of information relating to children. This is a matter of grave concern as information relating to children is sensitive data and must be handled and managed in a manner that protects the best interest of the child in line with Article 53(2) of the Constitution of Kenya. The framework should define the rights of a child in relation to personal data collected with consent of the parent or guardian when the child is still a minor and how the information is to be handled once the child turns eighteen particularly in light of the

https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

evolving capacities of children. It should also provide for special protections for the protection of children's biometric data collected under NIIMS.

f) Ensure Freedom from discrimination

Government should provide:

- Processes, procedures and mechanisms to fast track issuance of identity documents particularly to persons from communities or areas that have historically faced challenges in acquiring identification papers.

- Government should provide appropriate alternatives to the requirement of an ID or alien card, passport (for foreigners) as a precondition for enrollment of persons under NIIMS. This would help mitigate the high risk that persons from minority and pastoral communities will be excluded from legal recognition in Kenya.[192]

- Discrepancies regarding the issuance of ID cards need to be resolved before roll out of NIIMS or in the alternative Government needs to formulate a criterion for enrollment to NIIMS for persons who lack legal ID documents to at least enable them to access health care, access job opportunities and access mobile and financial services.

- The Government needs to provide a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework needs to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS.[193] The possibility of this exclusion is in itself not a sufficient reason to find NIIMS unconstitutional or in violation of the right to non-discrimination or equality before the law.

- Protect the data subject from discrimination, profiling, surveillance and identity theft.

- Restrict unauthorised access of the database and sharing of database information with third parties.

- Develop backups and redundancy features that ensure one is not locked out of NIIMS for factors which are beyond their control. NIIMS relies on biometrics and therefore persons with biometric features which make it challenging or impossible to authenticate are also likely to be excluded, such as labourers whose fingerprints wear out over time. This is important to ensure no segment of the population is unduly excluded from government recognition under NIIMS.

- Implement specific, proactive measures to recognize, cater for or even acknowledge persons who lack formal proof of identification.

---

192 "Kenya's New Digital IDs May Exclude Millions of Minorities," last modified May 12, 2020, https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

193 Ibid

g) Fast track recruitment and establishment of the Office of the Data Commissioner

The government should fast-track the recruitment of the Data Commissioner, the establishment of the office of the Data Protection Commissioner, as well as the recruitment or secondment of relevant staff who shall responsible for the implementation of the Act. Consequently, most of the sections in the Act cannot be implemented.

Once established the Office should spearhead the drafting of Data Protection Regulations under the Act and stakeholder engagement.

h) Spearhead and fast track required legal re-alignments

The Kenya Law Reform Commission should work with other stakeholders to amend existing laws to align with the Data Protection Act. These laws include: the Registration of Person Act, the Kenya Citizenship and Immigration Act, and the Registration of Births and Death Act to reflect the use of NIIMS. Also the National Assembly should prioritise debating any proposed amendments.

i) Embrace Privacy by Design in NIIMS

The government should embrace privacy by design principles in the infrastructural design and architecture of NIIMS.[194] This can be achieved by ensuring adequate data protection technical safeguards such:The separation of functions for identification and authentication and avoiding storage of transaction logs;[195] ensuring end to end data encryption; having a notification mechanism to inform parties as soon as possible that their data has been compromised;[196] use open software like India as opposed to a closed software system,[197] delinking Huduma Namba database from the Huduma Namba card, and embedding these protections in legislation. Emerging technologies such as cryptography and blockchain may also offer a solution that ensures the data on NIIMS is adequately secured and backed up.

j) Take adequate Cybersecurity measures

The government should ensure adequate security measures are taken: to protect the NIIMS database from cyber attacks; facilitate reporting of any data breaches by parties/agencies with access to NIIMS; and to facilitate reporting and resolving of any identity theft or duplication concerns.

Proper cybersecurity measures are required to ensure the security of personal data and sensitive data collected under NIIMS. The Interior Ministry should also conduct data protection impact assessments with regards to NIIMS and have protocols and procedures in place for management of cyber-attacks.

---

194 " Digital Identity:Prioritizing Human Rights," last modified May 13, 2020, https://unctad.org/meetings/en/Presentation/dtl_eWeek2018p15_WafaBen-Hassine_en.pdf

195 Ibid

196 Ibid

197 "Nubian Rights Forum & 2 others v Attorney General & 9 others," last modified May 14, 2020, http://kenyalaw.org/case-law/cases/view/189189/

k) Adopt Transparent Communication and Reporting

The government should be transparent and provide access to information regarding NIIMS in keeping with best practices. For example, Estonia provides a blueprint for transparency by the Executive leading to trust and increased use and uptake of digital IDs. Consequently, mechanisms should be provided to ensure The public is informed:

- who has access to their data,
- how their data is being used,
- the right to object to processing and to have their data corrected or expunged from the system, and,
- the right to be informed and to institute any legal proceeding against the government in case the data is compromised.

5.2.3 Private Sector

The private sector is a key stakeholder in the public-private multi-stakeholder environment in which Huduma Namba will be used.

a) Be Data security champions, innovators and solution providers

Private sector is the lead technology innovation stakeholder group as well as the lead technology solution supplier in matters technology. The sector should continue developing technology products and solutions, offering services as well as participating in data security awareness raising campaigns. One key role of the sector is to lend technical expertise and solutions to the Government in the implementation and protection of NIIMS.

The private sector should work with the government and where possible share their expertise with the government on the best practices regarding use and maintenance of data and database systems. Private sector can also provide solutions such as cloud storage for purposes of storing the Data on NIIMS as well as any other relevant technology or technology based solutions.

b) Engage in regulatory reform process

The private sector should continue engaging in the regulatory reform process regarding uptake of Huduma Namba and make contributions to secure a robust legal framework that enables business operations to continue even with the adoption of digital identification in Kenya.

The private sector is part of the largest community of service providers that will be affected by the adoption of digital ID technology and systems in Kenya. It is imperative for the sector to contribute towards the laws guiding the implementation of NIIMS as well as provide the Government with information required to facilitate business and service delivery within the digital ID ecosystem.

c) Provide access to services without discrimination

In providing services to the public, the private sector players should only require identification in accordance with the law and refrain from unnecessarily burdening the public or requiring excessive identification information.

In relation to Huduma Namba, the private sector should continue rendering essential services such as health and education to persons, irrespective of whether or not they are registered for Huduma Namba. Huduma Namba remains optional and therefore Kenyan citizens and residents should not be denied services by private sector players for lack of Huduma Namba or any other digital identity adopted by Government unless such denial of service is provided for in law.

d) Abide by data protection principles

Any private company integrated to NIIMS or with access to the NIIMS database should manage all personal data accessed in keeping with the data protection principles under the Data Protection Act 2019. NIIMS data should not be commercialised or used for undisclosed or unregulated profit making ventures.

5.2.4 Civil Society Organisations

Civil Society Organisations (CSOs) play a key part in defending human rights and holding Governments and private businesses accountable. They should:

a) Advocate for digital rights

CSOs should continue being at the forefront of advocating for the respect of human rights and the implementation of NIIMS in a manner that respects all human rights. If not for the actions of CSOs, the implementation of NIIMS would have negatively impacted many Kenyan citizens. It is civil society groups that led in filing petitions in the Huduma Namba case leading up to court orders for NIIMS enrollment to be voluntary as well as orders restraining further roll out in the absence of a proper data protection framework. They should continue advocating for respect of digital rights through various effective processes including litigation where appropriate.

b) Monitor NIIMS Implementation

CSOs should continue monitoring the implementation of NIIMS and raising all relevant human rights concerns with the relevant stakeholders for redress. In many ways CSOs have kept the government and private sector in check by voicing human rights concerns which in some cases addressed. CSOs should remain vigilant to ensure that the data on NIIMS is not used to target or discriminate against any group, persons or vulnerable populations.

CSOs should also monitor whether NIIMS data is used for its intended purposes and not to benefit certain entities in government or the private sector.

c) Engage in regulatory reform process

CSOs should continue engaging in the regulatory reform process regarding uptake of Huduma Namba and make contributions to secure a robust legal framework that ensures the respect and preservation of human rights (and particularly the right to privacy) and continue even with the adoption of digital IDs in Kenya. It is imperative for the sector to contribute towards the laws guiding the implementation of NIIMS as well as develop draft legislative proposals and input relating to law and policy reform, to ensure human rights are respected in service delivery within the digital ID ecosystem.

5.2.5 Citizens

a) Hold government accountable

The citizens also have a role to play in ensuring that NIIMS is a success. Citizens should hold the government and their elected leaders accountable in relation to the processing of personal data as well as the rights and obligations provided under the Data Protection Act. Citizens should require and demand transparency from the government in relation to NIIMS and seek legal action if the government:

- Fails in providing adequate protection for NIIMS;
- discriminates based on information in NIIMS;
- if there is a data breach on NIIMS, identity theft or identity duplication;
- denies them essential services for lack of Huduma Namba when enrollment is voluntary; or,
- otherwise contravenes the law.

b) Engage in regulatory reform process

Citizens should engage in the regulatory reform process regarding uptake of Huduma Namba and make contributions to secure a robust legal framework that ensures the protection of citizen rights even as the government adopts digital IDs in Kenya.

It is imperative for the citizens to contribute towards the laws guiding the implementation of NIIMS as well as provide the Government with input relating to law and policy reform, to ensure citizen rights are preserved in service delivery within the digital ID ecosystem. Members of the public who have the requisite ICT skills should contribute in identifying, informing and patching any security vulnerabilities in the system.

The citizens should be vigilant to ensure that the government does not sell off their data to private entities for economic benefits and remain vigilant with documenting and reporting issues and enforcing citizen rights.

5.2.6 Media

a) Communication and reporting

Stakeholders in the media sector should play their role in guarding the public interest through objective reporting on the Huduma Namba and the NIIMS system. The media is one of the most critical stakeholders in realization of the right to access information. Citizen rights, important information, unfair government practices and well grounded complaints with regard to digital IDs should be adequately ventilated in the media.

Access to and provision of relevant information should involve a multi-stakeholder collaboration between the media, technical community, government, private sector etc.

5.2.7 Technical Community

a) Lend expertise

The technical community has a vital role to play in ensuring that NIIMS is regularly tested in order to identify vulnerabilities in the system. Its unique knowledge in cybersecurity and data protection should be utilised in generally improving the system through collaboration with the relevant government MDAs, Private Sector, Academia and CSOs.

5.2.8 Academia

a) Research

The role of academia is to conduct high quality research on the social, economic, scientific, legal and any other impacts of Huduma Namba as well as to contribute to a vast pool of knowledge on the system. This will provide a good basis for policy makers as well as future researchers on identification systems in Kenya and any needed practical, legal, technical interventions.

KICTAnet
KENYA ICT ACTION NETWORK