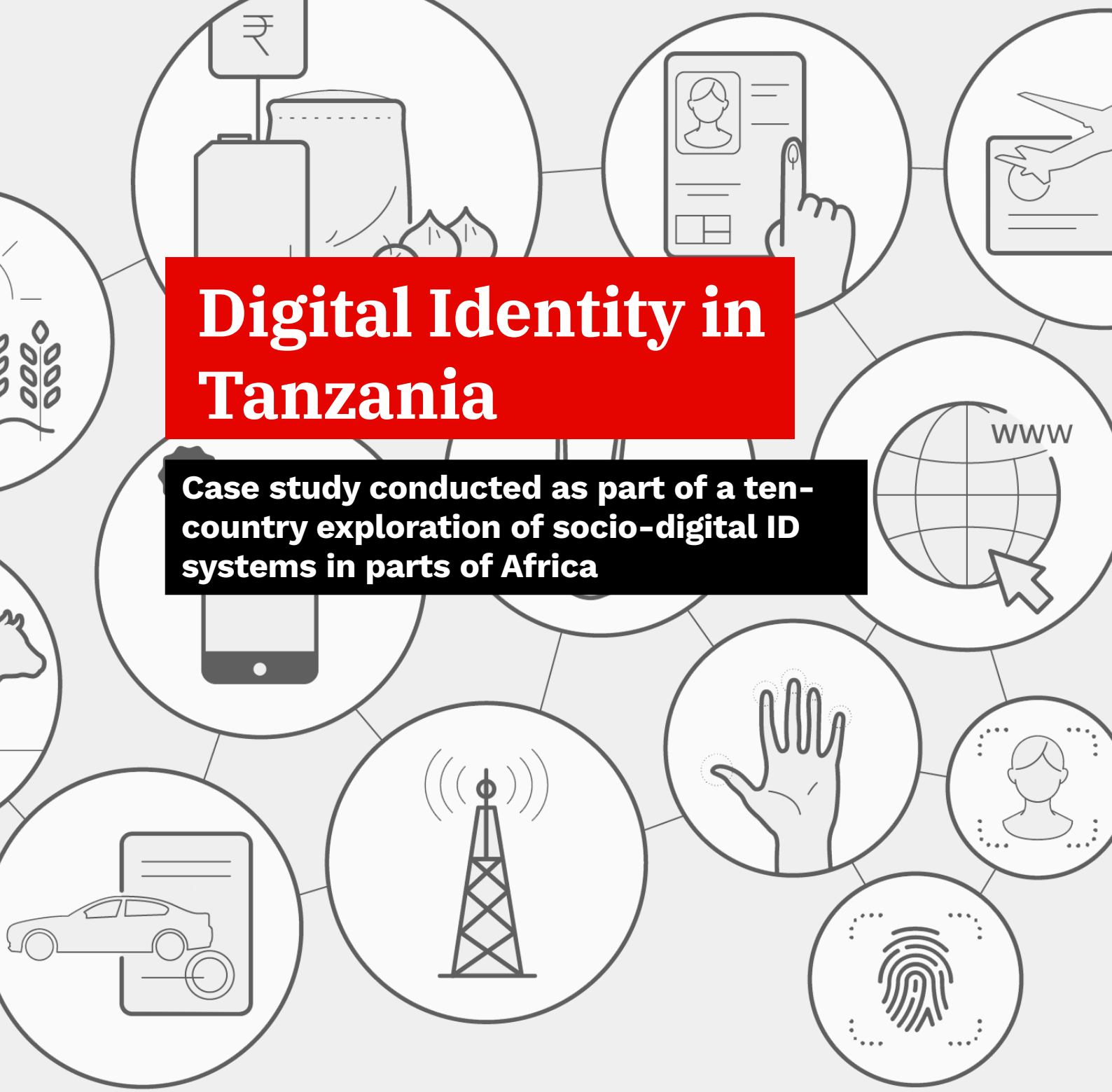

Digital Identity in Tanzania

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

RESEARCH & WRITING
Dr Patricia Boshe

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

COPYEDITING
Samantha Perry

COVER ILLUSTRATION
Akash Sheshadri

LAYOUT
Aparna Chivukula

RESEARCH ICT AFRICA

THE CENTRE FOR internet & society

OMIDYAR NETWORK™

Digital Identity in Tanzania

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

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

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

Digital Identity in Tanzania

By Dr Patricia Boshe, African Law and Technology Institute (AFRILTI)

PREAMBLE

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

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

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

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

2 Martin, Schoemaker, Weitzberg & Cheesman, 2021.

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

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

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

The Project

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

3 Breckenridge, 2014.

4 African Union Commission, 2021.

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

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

systems in Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe.

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

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

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

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

PREAMBLE REFERENCES

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

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

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

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

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

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

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

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

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

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

ACKNOWLEDGEMENTS

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

ABSTRACT

The **Universal Declaration of Human Rights** (UNGA, 1948) declared the right for everyone to be recognised as a person before the law. On this basis, international organisations and countries around the world have devised initiatives and systems to promote and ensure everyone is identified and legally recognised as a person.

Identification systems (ID system) created for this purpose provide individuals with some form of an identity artefact (such as a card) containing personal identification information. The identity artefact gives a person not only a legal identity but also facilitates individual access to civic services.

This research evaluates the ID system in Tanzania, the National Identity Authority (NIDA). The identification and registration process are still ongoing, with about 74% of the eligible population registered. However, the overall evaluation of the NIDA ID system shows a potential exclusion to civic services, system insecurity, insufficient protection framework and lack of redress system.

To avoid exclusion, it is recommended that the government reconsider its objective in making NIDA IDs exclusive IDs, instead allow the use of other functional IDs parallel with the NIDA IDs. It is further recommended that the law governing the ID system be reviewed to improve the security and protection framework.

ACRONYMS AND ABBREVIATIONS

AFIS	Automated Fingerprint Identification System
CAG	Controller and Auditor General
ICT	Information and Communications Technology
ID4Africa	Identity for All in Africa `
ID4D	Identity for Development
MoU	Memorandum of Understanding
NEC	National Electoral Committee
NGO	Non-Governmental Organisation
NIDA	National Identification Authority
NIN	National Identification Number
RFID	Radio Frequency Identification Technology
RITA	Registration, Insolvency and Trusteeship Agency
RZRA	Registrations of Zanzibaris Resident Act
SIM (card)	Subscriber Identity Module (card)
TCRA	Tanzania Communication Regulatory Authority`
TIN	Tax Identification Number
Tshs	Tanzanian Shillings
ZanID	Zanzibar Identity Card

LIST OF FIGURES

LIST OF TABLES

CONTENTS

INTRODUCTION

1.1 OVERVIEW

The UN Sustainable Development Goals (SDGs), adopted in 2015, are geared to "provide legal identity to all, including birth registration, by 2030" (Goal 16.9). It is estimated that 987 million people globally are currently without legal identity[9] (down from 1.8 billion in 2016), hampering their access to healthcare, education systems, and governmental services.[10] Communities from low-income countries have the greatest portion of their populations without legal identification (an estimated 45% of women and 28% of men lack a legal ID).[11] This discrepancy has led to global strategic efforts to build capacity and hasten the provision of legal identities for all.

In response, the World Bank and other stakeholders launched the Identification for Development (ID4D) initiative in 2014 to help countries realise the transformational potential of digital identification systems to achieve the SDGs.[12] In 2016, the United Nations Office for Partnerships hosted the ID2020 Summit – *Harnessing Digital Identity for the Global Community*, at the United Nations in New York. The Summit brought together stakeholders from the public and private sectors, policy analysts and non-governmental agencies, to work together in the quest to provide legal identity to all vulnerable and invisible people by 2030.

Africa, and Sub-Saharan Africa in particular, has the highest prevalence of adults without legal identity in the world. The World Bank estimated in 2017 that less than a third of adults in Sub-Saharan Africa lack a legal identity, [13] the highest of any global region. In addition, the coverage of legal IDs in Sub-Saharan Africa is not uniform, as it ranges from a low of 21% in South Sudan to the almost universal coverage in Botswana and South Africa. To help the region realise

9 WEF, "A Billion People have no Legal Identity - But a New App Plans to Change That", World Economic Forum (2/22/2021); *https://www.weforum.org/agenda/2020/11/legal-identity-id-app-aid-tech/* accessed on 22 February2021

10 United Nations Office for Partnerships, "ID2020 Summit 2016" *https://www.un.org/partnerships/news/id2020-summit-2016* accessed on 19 February 2021.

11 WEF (Supra).

12 The World Bank, "Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey", at page 1: The report is available at *http://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf* accessed on 22 February 2021.

13 *Ibid*, p. 4.

uniform universal legal identification for all people, the initiative *Identity for All in Africa* (ID4Africa) was founded in 2014. This NGO reportedly helps African nations on their journeys to "develop robust and responsible Identity ecosystems in the service of development and humanitarian action".[14]

This report examines Tanzania's efforts to develop and provide legal identity to citizens and residents. The assessment is limited to foundational identity systems (as opposed to functional identity systems). In this case, this means the National Identity issued by the National Identity Authority (NIDA), and in a limited scope, the Zanzibar Identity system (ZanID).[15]

METHODOLOGY

The research employed qualitative assessment of laws and the legal framework for the identification and registration of citizens in Tanzania mainland and Zanzibar. Other reports and related documents were also reviewed to understand the background information, initial development and the actual implementation of the NIDA system. This was largely a desk review of documents relating to the ID system in Tanzania and included public websites for the National Identification Authority and the Parliament of Tanzania website. Additional information was obtained from online news agencies (e.g. newspapers) which have captured ID system development through the years since Tanzanian independence in 1961.

14 ID4Africa, "Identity for All in Africa", at *https://id4africa.com/* accessed on 2 February 2021.

15 In Tanzania the NIDA IDs are issued to both citizens and residents in Tanzania Mainland and Zanzibar. NIDA IDs are the foundational IDs in Tanzania. The Zanzibar ID system is brought into the discussion because it is a system for registration and identification established for the Zanzibaris. In practice, it existed before the NIDA system and it currently operates parallel with the NIDA ID system.

1.2 IDENTITY ECOSYSTEM IN TANZANIA

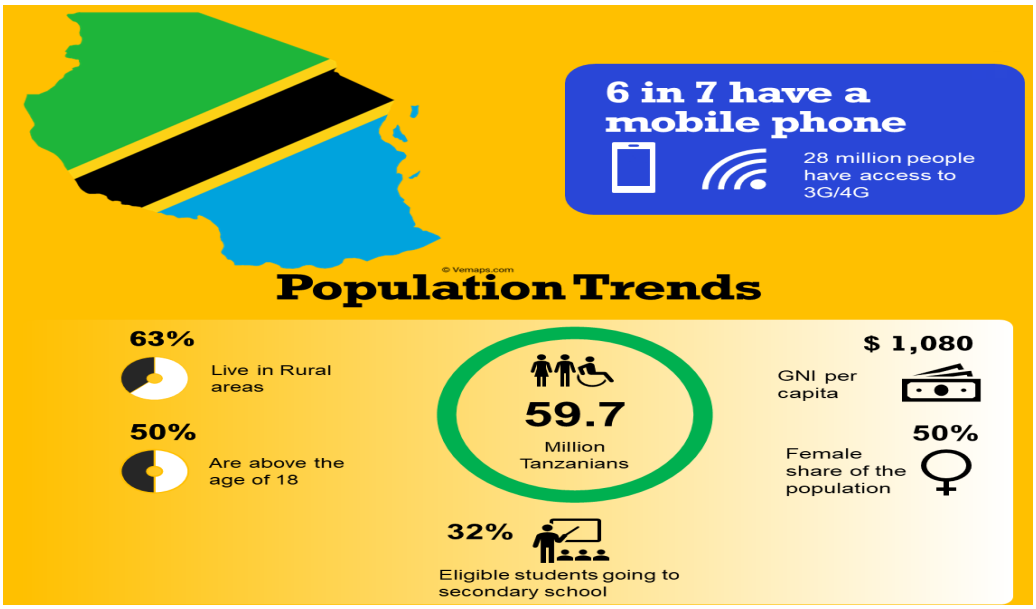

Figure 1: Tanzania Profile (Data Source: World Bank, 2021)

Tanzania began conceptualising the idea of national identification for its people right after Tanganyika's independence in 1961 and the subsequent unification with Zanzibar in 1964. As far back as 1965 Tanzania's first president, the late Julius Kambarage Nyerere, emphasised the need to establish a national identity for the citizens of the new country (Tanzania).[16] However, it was never implemented due to financial and capacity constraints.

Meanwhile, in Zanzibar identity cards for citizens have existed since the early 1960s. In 1986, the parliament of Tanzania enacted the Registration and Identification of Persons Act (RIPA) to facilitate the registration of persons in the United Republic of Tanzania and to issue them with identity cards.[17] Again, no national effort was successful at the time in providing legal identity cards for Tanzanians and residents. This legislation, however, spelt the end of the Zanzibar identity cards which were, as a result, abolished in the early 1990s in an effort to strengthen the Tanzanian Union.[18]

16 Stamp, "Zanzibar and Tanzania #330 (1965)", at *https://stampaday.wordpress.com/2018/02/07/zanzibar-and-tanzania-330-1965/* accessed on 22 February 2021.

17 Act No No.11 of 1986.

18 UNPO, " Zanzibar: All Adults Must Carry Identity Cards by 1 April", *https://unpo.org/article/3884* accessed on 23 February 2021.

In 1997, the Government of Tanzania (GoT) reportedly entered into negotiations with a British firm, Ms/Reginal Service, to produce the nation's first identity cards.[19] These negotiations, however, came to nought. Once again, Zanzibar was the first to act and introduce the Registrations of Zanzibari Residents[20] in 2005 leaving Tanzania Mainland behind. This Act made it mandatory for the island's residents aged 18 years and above to be registered and to acquire an ID.[21] Additional eligibility was pursuant to being a citizen of Tanzania and resident in Zanzibar for at least 10 years.[22] Failure to register without valid reasons would lead to a jail term of one year, a fine of Tshs 100 000 (the equivalent of USD 100), or both.[23] The Act further requires all Zanzibaris residing outside Zanzibar – upon turning 18 years of age – to attend to the registrar office for registration.[24] The Act also makes it an offence to discourage others to register.[25]

The Zanzibar government started to register persons and issued a projected 450,000 eligible Zanzibaris with national identity cards (known as ZanID). As 2005 was an election year, the opposition party raised concerns about the process and use of personal data, alluding to how both the process and personal data collected are vulnerable to misuse for political gain. Eventually, the first ID card was issued on 16 July 2005 to the then President Karume.[26] By March 2006, around 480,000 Zanzibaris had been registered, with 445,000 people having received their ZanID. The relatively fast pace of registrations and dissemination of cards was largely due to the government making registration mandatory and limiting access to several social services to only those with ZanIDs.[27]

In 2006, Tanzania Mainland commissioned a feasibility study for the national identification and registration of persons in Tanzania. The study drew an implementation roadmap to enable the successful introduction and

19 Merere. A, "Tanzania IDs on Hold as Negotiations Drag on", *The East African Newspaper*, 2nd April 1998

20 Act No.7 of 2005.

21 Sections 6(i) and (ii) and 10(i) of the Registrations of Zanzibaris Residents Act No.7 of 2005.

22 *Ibid*, Sections 12 and 15(a).

23 *Ibid*, Section 14(1)(a).

24 *Ibid*, Section 8.

25 *Ibid*, Section 14(3) - an offence punishable by a prison term not exceeding six months.

26 Fewer Africa, "Electoral Violence and Reconciliation Zanzibar", Nairobi, 2008; *https://reliefweb.int/sites/reliefweb.int/files/resources/E3DB1AAD353D4D3649257046001A4BC7-fewer-tza-20jul.pdf* accessed on 23 February 2021.

27 "Rush for IDs in Zanzibar", The New Humanitarian (4/3/2006) *https://www.thenewhumanitarian.org/report/58639/tanzania-rush-ids-zanzibar* accessed on 23 February 2021.

implementation of a national identification system in Tanzania.[28] Consequently, in 2008, the president of the United Republic of Tanzania established the National Identification Authority (NIDA).[29] However, it was not until 2011 that RIPA was enforced by Government Notice No. 257A.[30]

NIDA is tasked with identifying and registering citizens and legal residents in Tanzania – both Mainland and Zanzibar[31] – and issuing them with National Identity Cards.[32] Other than the Registrations of Zanzibaris Resident Act (RZRA), RIPA does not explicitly make it a mandatory requirement for a person to have an ID. Section 7(1) uses the words, "[E]very person of above the age of eighteen years (...) may make an application for registration in pursuant to this Act". However, read together with a set of regulations that are supplementary to RIPA - the supplementing Regulations of 2014 - identification and registration appear to be mandatory.[33] In addition, Section 20 makes it an offence if a person fails or refuses to comply with either Section 7 (above) or Section 9, which requires individuals to submit a fingerprint, a signature, and furnishing of personal information to the Registrar. The 2014 Regulations go further by imposing a duty on local authorities to ensure all persons within their jurisdictions are registered.[34]

By implication, these provisions make the ID mandatory; the aim being to provide all citizens, legal residents, and refugees who are older than 18 years of age (about 25 million individuals at the time of writing) with contactless, multipurpose identity cards.[35] The registrations (the national identification exercise) started in 2013, with then President Jakaya Kikwete being the first

28 Nagai. Melamari Simon, "The Challenges and Need of Legal Frameworks for Data Protection in Tanzania: Case Study of Tanzania National Identification Authority (NIDA)", Master's Dissertation, Open University of Tanzania, Dar es Salaam at page 2. Dissertation available at *http://repository.out.ac.tz/1061/1/Nagai_Melamali.pdf* accessed on 22 February 2021.

29 By virtue of his constitutional powers (Article 36) and Section 2(1) of the NIDA Establishment Instrument of 2008 (Government Notice No. 122 of 2008) which reinforces Section 5 (1) of the Registration and Identification of Persons Act No.11 of 1986.

30 Nangai, (*supra*), p. 27

31 Section 4(1) of the Act No.11 of 1986.

32 See Sections 7, 8 and 10 of the Act No.11 of 1986.

33 Section 4(1) of the Regulation uses the words "shall" instead of "may", as in the Act. In addition, Section 4(2) makes a requirement that the registration must be made within 90 days from the date of attaining the age of eighteen.

34 Regulation 14 of the Registrations and Identifications of Persons (General) Regulations, 2014.

35 The World Bank, "The State of Identification Systems in Africa", at page 53 *https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y* accessed on 22 February 2021.

Tanzanian to receive a national identity card.[36] The NIDA card is a 80kb near-field communications (NFC) smart card with contactless technology that can be used as a mobile wallet, and its implementation makes Tanzania one of the two countries in Africa with advanced identification technology.[37] Authentication is mainly through fingerprints. The initial launch cost was an estimated USD 160 million and IDs are provided to citizens free of charge.

With this in mind and the achievement made so far, there is a good chance that Tanzania will meet the 2030 vision of providing legal identity to all vulnerable and invisible people. However, an important aspect is overlooked; there is lack of a clear and sufficient rights protection and redress system. On the one hand, the laws have neither rules nor procedures for an individual to enforce their rights, specifically rights to data protection and privacy. On the other hand, the laws protect NIDA officials from prosecution in case of mishandling of data. In addition, Tanzania has no comprehensive data protection law or framework. This leaves individuals with no recourse in case of rights violation.

THE PROCESS

The process begins with production of documents by an individual wishing to be registered and issued with the NIDA ID. The 2014 Regulation stipulates required documents – depending on an individual's residence status. Here, the Regulation provides for two categories, citizens of the United Republic of Tanzania, and alien residents (including diplomats and refugees). The table below shows documents listed under Regulation 5 (3) as preregistration documents for the above-mentioned groups.

36 Makoye. Kizito, "Tanzania Launches New ID Cards to Combat Election Fraud", Thomas Reuters (2/22/2021) Available at *https://news.trust.org/item/20130227092500-jm6av/* accessed on 22 February 2021.

37 Another country with advanced ID technology is Nigeria. See World Bank Group, The State of Identification Systems in Africa: a Synthesis of Country Assessment, p. 43 and 53

Citizen of the United Republic of Tanzania	**Alien Resident**
Birth certificate or written evidence of birth, and	Passport
Primary School Leaving Certificate or Form Four Leaving Certificate, and	Birth certificate
Birth certificate or affidavit of birth or written evidence of birth of either or both parents or grandparents, or	Residence permit, in case of a refugee, a refugee ID card or ration card.
Passport of either of both of his parents, and	Such other particulars as the Minister may determine
Voter's Card (for Zanzibar: ZanID) or Driver's license	
Such other particulars as the Minister may determine	

Table 1: Registration documents

An individual being registered by NIDA receives a 20-digit unique identifier number called a National Identification Number (NIN). The NIN is linked to a single set of biometric attributes of the individual, has no expiry date, and cannot be changed or altered in any way.[38] NIDA utilises an Automated Fingerprint Identification System (AFIS) in an effort to avoid mistakes or duplicates. AFIS works by automatically matching single or multiple unknown fingerprints against the samples contained in the National ID database registry. Verification is done for all new applicants by passing their records through AFIS to establish if matching records already exist. Once the information is verified, applicants can be issued their National ID smartcard . Processed information is stored centrally within a data centre which is connected to all district registration offices via the national ICT broadband backbone. The data centre conforms to ISO 27001 (information security management) and ISO 9001 (quality management).[39]

38 Fernmelde-Union, Internationale. "*Digital identity roadmap guide*", Geneva: International Telecommunication Union, 2018, p.53

39 *Ibid.*

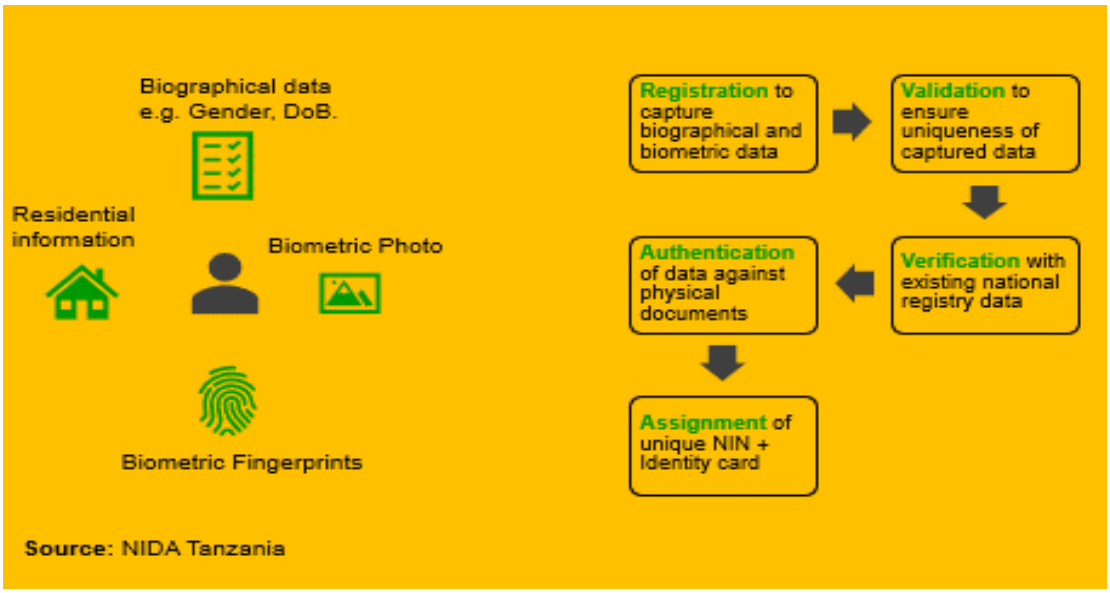

Figure 2: Summary of the identification and registration process. (Source: NIDA Tanzania)

SITUATION ANALYSIS: IDENTIFICATION AND REGISTRATION OF PERSONS IN TANZANIA

From 2013 to 2015, about 6.5 million residents were registered from seven regions; with only 2.7 million of the registered residents receiving their national ID cards. In 2016, as the first batch of national IDs were handed out, recipients complained about the poor quality of the IDs, especially the illegible signatures, which rendered most of the IDs unacceptable by several financial providers. This led to the President criticising and eventually firing the director-general for NIDA, with a new acting director ordering a recall of over two million ID cards.

Overall, the speed of the registrations was also slower than expected, which led to the government implementing additional measures to increase registrations. Two of the most impactful measures were the partnership between NIDA and the National Electoral Committee (NEC) and the mandatory registration of SIM cards using the national ID information. The NEC was able to identify and remove duplicate data for approximately 22.7 million voters and issued new biometric voter ID cards in time for the 2015 national elections. Eventually, in 2016, NIDA used the NEC database to import individual voter records and pre-registered around 90% of the population.[40] NIDA also "borrowed" 8 000 biometric registration machines from the NEC to use across its 150 district registration offices and thus increase their capacity to register ID applicants.

40 World Bank 2017 (*supra* n. 27) p. 53

SIM registration also played a role in take-up. In 2018, Tanzania made it mandatory for SIM users to register their SIM cards using their NIDA IDs. Initially, an individual could register SIM cards using any kind of an ID including voter card, passport or driver's licence.[41] The Tanzania Communication Regulatory Authority (TCRA) later announced that only NIDA IDs could be used for SIM card registration, however, and issued a deadline for the SIM registration (biometrically registered with the NIN) on 1 May 2019.

An initial deadline of 31 December 2019 was set for mobile users to register the SIM cards, or face disconnection. Only 42% of all SIM card owners were able to biometrically register by the deadline, and the government extended the deadline to 20 January 2020 to avoid mass switch-offs of mobile users.[42] In the same year, the government adopted a Regulation[43] making NIDA IDs the exclusive ID cards for the SIM card (re) registration process.[44] As a result, more people registered with NIDA to avoid SIM deactivation.

NIDA IDS FOR WELFARE DELIVERY

Making the NIDA ID an exclusive ID to access services – including government employment[45] – increased the number of biometrically registered persons from 6.1 million in 2015 to 15.2 million (just over 50% of all eligible persons) at the end of 2017.[46]

It was soon realised that NIDA, under RIPA, is only mandated to register and

41 In Tanzania, SIM cards are subject to registration under the Electronic and Postal Communications Act (EPOCA)Act No. 3 of 2010. Under Section 131 of the Act, it is an offence to use an unregistered SIM card. An offence that attracts a penalty of a prison term not exceeding three months or 500,000/- See also, Mwangonge. Henry, "Tanzania Begins Biometric Registration of Mobile Users", The Guardian (22 February 2021); *https://www.ippmedia.com/en/news/tanzania-begins-biometric-registration-mobile-users* accessed on 22 February 2021.

42 Global Voices Advox, "Deadline looms for biometric SIM card registration in Tanzania", 22 January 2020; *https://advox.globalvoices.org/2020/01/08/deadline-looms-for-biometric-sim-card-registration-in-tanzania/* accessed on22 February 2021.

43 Electronic and Postal Communications (SIM Card Registration) Regulation, GN. No. 112 of 2020.

44 See Regulation 4 of the Electronic and Postal Communications (SIM Card Registration) Regulations, 2020.

45 See Tanzania government recruitment portal at *http://portal.ajira.go.tz/* and the Recruitment Portal User Guide v 2.0 Main Change together with the Recruitment Portal User Guide v 2.1 both available at the recruitment portal above.

46 Burt. C, "Tanzania Leverages Increased Knowledge and Skill to Move toward Universal Biometric Identity" in BiometricUpdate.com, 2018, *https://www.biometricupdate.com/201805/tanzania-leverages-increased-knowledge-and-skill-to-move-toward-universal-biometric-identity* accessed on 22 February 2021.

issue identity cards to Tanzanian citizens and eligible residents aged 18 years and older.[47] This would mean exclusion of services such as the use of mobile phones,[48] student loans, or even public employment[49] to people under the age of 18. In 2020, the Minister for Home Affairs addressed the Parliament regarding the Ministry's plan to issue NIN to citizens and residents below 18 years of age, thus expanding the registry database even more.[50] In addition, NIDA is working on integrating the civil registration system with the goal of possibly issuing national ID numbers to newborn babies at the time of their birth registration (extending its coverage from birth), which will be done in partnership with the Registration, Insolvency and Trusteeship Agency (RITA).[51]

To harmonise NIDA and the ZanID systems, the government launched the process of digitising the ZanID in 2018. Previously, the ZanIDs held no biometric information, making it difficult to integrate with the NIDA database.[52] Currently, NIDA is already fully integrated with Zanzibar's civil registry, ensuring registration information from the island residents are accessible to NIDA. As RITA is increasingly undertaking its digital transformation roadmap, it is integrating with NIDA for the Tanzania mainland. The goal is reportedly to allow the assignment of NINs to new birth registrations across both Tanzania mainland and Zanzibar.[53]

The identification and registration of eligible persons will continue to see constant advancement due to policies that have made it mandatory to access a series of public services via digital identity. This includes obtaining a Tanzanian passport, opening or registering a new company, registering a SIM card, and for tax purposes, e.g., obtaining a tax identification number (TIN).

This is a significant shift of procedure, as previously a person would have to separately provide biometric and biographical information to each of these entities when requesting services, e.g. passports. NIDA has merged the Tanzanian

47 Peter. F, "Tanzania: Kids Lined up for NIDA Numbers. The Guardian (19 February 2021); *https://citizenshiprightsafrica.org/tanzania-kids-lined-up-for-nida-numbers/* accessed on 19 February 2021.

48 Currently, parents and guardians are allowed to register SIM cards for their under-age children.

49 In Tanzania, a person of 14 years is allowed to work. Section 4 of the Employment and Labour Relations Act (ELRA), 2004 defines a child as a person under the age of 14 years but for the purpose of employment in hazardous sectors, it is defined as a person under the age of 18 years.

50 Peter. F, (*supra*)

51 World Bank 2017 (*supra*), p. 53

52 Zanzibar Civil Status Registration Agency (ZCSRA), "Wazanzibari Sasa Kutambuliwa Kidigitali (E-ID Card)', *https://www.zcsra.go.tz/resources/view/wazanzibari-sasa-kutambuliwa-kidigitali-e-id-card* accessed on 8 March 2021.

53 ID4Africa, (*supra*).

ID scheme space, which was very fragmented, with multiple overlapping and incompatible identity systems across governmental agencies. Previously, each ministry had distinct registration requirements, infrastructure, identification, and verification processes. This suggests, although it was not publicly declared, a synchronisation of government databases that contain individual personal data, including biometric data with NIDA as the central data point.

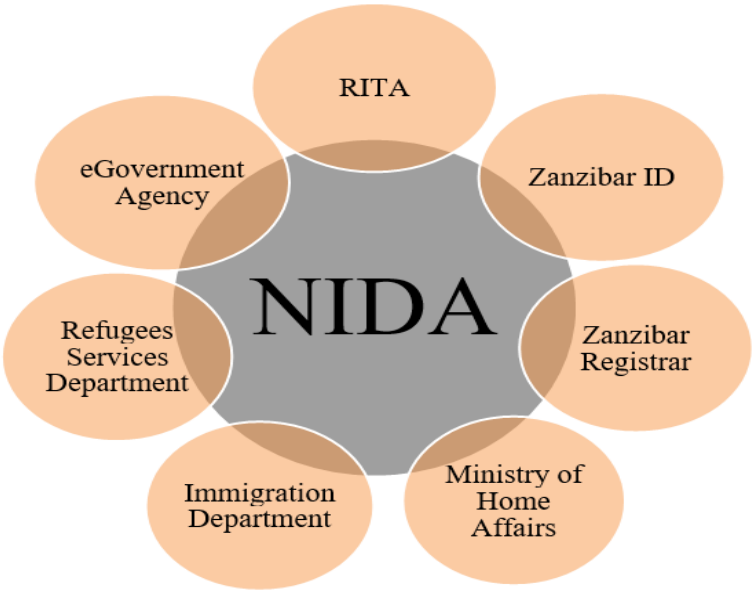

Figure 3: A work in progress for NIDA IDs.
(Source: Ministry of Home Affairs)

According to the Ministry of Home Affairs, NIDA had registered 21.8 million NIN by March 2020. This is an increase of 2.5 million NIN registrations between July 2019 and March 2020.[54]

Unfortunately, the speed of registering applicants has not been matched by the speed of issuing the electronic identity cards. Just about 6.1 million registered persons have so far received their physical IDs. This is far below the targeted goal of issuing national IDs to 24 million people by the end of the 2019/2020 fiscal year.

The government set two ambitious goals for the 2020/2021 fiscal year: to issue 6.1. million NINs, bringing the total to 27.8 million registered persons, and to produce 18 million national identification cards. The government expects to procure new modern machines to ensure this target is met.[55] At the same

54 Peter. F, (*supra*).

55 Peter. F, (*supra*).

time, NIDA is working on expanding its capacity by establishing offices in 150 of Tanzania's 169 districts. As of 2017, there were 142 registration centres functioning across Tanzania.[56] As of June 2021, there are 160 registration offices nationwide,[57] surpassing the set goal of 150 offices.

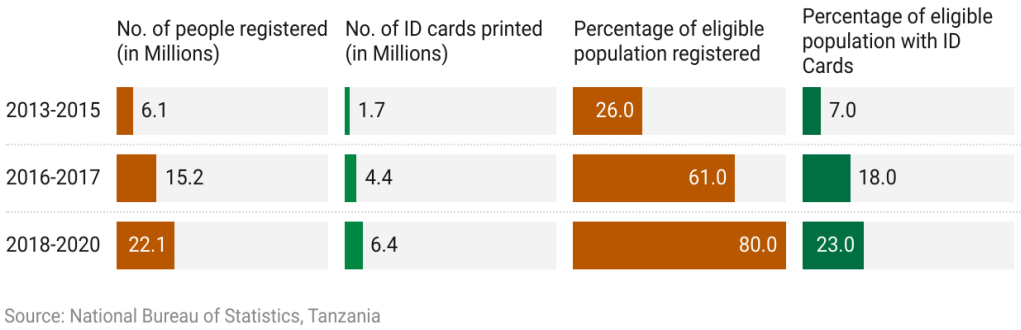

Figure 4: Status of registrations in Tanzania
(Source: National Bureau of Statistics, Tanzania)

CHALLENGES IN IDENTITY CLAIM

Tanzania currently recognises three types of citizenship: by birth,[58] by descent,[59] and by registration or naturalisation.[60] The pre-registration process has proven a challenge to citizenship by birth and by descent, as a vast majority of the adult population of Tanzania have no birth certificates and are thus unable to provide documentation to claim their identities in the registration process. It is estimated that only 50.2% of all births in Tanzania take place at medical facilities and that the birth registration rate for children under the age of five years is 16.3%.[61] According to the 2012 census, an estimated 85% of the population did not have a birth certificate.

Although according to the 2014 Regulation a person can provide "evidence of

56 World Bank 2017, (*supra*).

57 Vituo vya Usajili NIDA: *https://nida.go.tz/swahili/index.php/vituo-vya-usajili/*

58 Section 4(1) and 5(1) of the Tanzania Citizenship Act, No. 6 of 1995.

59 *Ibid*, Section 4(3) and 6.

60 *Ibid*, Section 4(2).

61 World Bank 2017 (*supra*).

birth" to prove their citizenship[62], without a birth certificate, it is still difficult for someone to adequately prove citizenship of Tanzania in accordance with the Citizenship Act. RITA, the agency issuing birth certificates, also does not have offices in all districts in Tanzania, making it harder for rural communities to access their services. This is despite the Under-Five Birth Registration Initiative (U5BRI), an initiative launched by RITA in 2012. The initiative increased the number of birth registrations points from 183 districts to ,817 within 1 736 ward offices and 3 081 health facilities, but is only implemented in 13 out of the 26 regions in Tanzania.[63]

In addition, a significant number of citizens born or residing near the country's borders have reportedly had their citizenship or nationality questioned. This is most likely because the Tanzanian borders are porous, with interconnected communities on both sides of the borders. In fact, in 2020, the Prime Minister defended the strict identification and registration processes being introduced to communities residing near the national borders as they are easily penetrable by foreigners who can effortlessly mingle with the local population.[64] Other challenges include the need to build capacity and improve ICT infrastructure for district registration offices, the outdated legal and regulatory framework, and the co-existance of fragmented identity ecosystems. Another concern is the time and money spent by applicants to physically go to registration centres, which can be a considerable distance from their homes.

ANALYSIS OF TANZANIA'S DIGITAL ID SYSTEM

This assessment looks into the legitimacy and robustness of the ID system in Tanzania. The assessment evaluates the law establishing and mandating NIDA and corresponding regulatory framework(s) to support the purposes of the law, while at the same time protecting individual users of the NIDA ID. The assessment is conducted on three levels: the first is the rule of law test, the second is the rights-based test and the third is the risk-based test.

62 According to Regulation 5(5) of the Regulation, an evidence of birth "means a prescribed form issued by the Village/Mtaa Council to an applicant for purposes of determination and verification of his birth place, residence, identity and other matters of similar nature".

63 Sanga *et al* 2020.

64 "Tanzania: PM: Tight ID Card Filing in Border Regions Right", The Guardian 2020 at *https://citizenshiprightsafrica.org/tanzania-pm-tight-id-card-filing-in-border-regions-right/* accessed on 19 February 2021.

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

The issuance of IDs is governed by RIPA and its 2014 supplementing Regulations. This law and the Regulations apply to both Tanzania Mainland and Zanzibar. In addition, Zanzibar has the Registration of Zanzibaris Resident Act (RZRA) and the Zanzibari Act which governs the issuance of IDs. These laws apply only to Zanzibaris. RIPA defines an ID card as "a card indicating the identity of the holder issued by the Registrar".[65] Just to bring in the context, this law was adopted in 1986, by that time neither NIDA nor the idea of digital ID existed. In 2014, Tanzania issued supplementing Regulations to the 1986 Act. In these Regulations, an ID card is defined as "a card which is issued by the National Identification Authority". [66] In Zanzibar, Section 2 of the RZRA defines an ID card as "a certificate of identity issued to a Zanzibari resident under Section 10 of this Act". Other than a definition of a "chip" in the Regulations, there is no explicit statement to the effect that the ID cards issued under either of the two laws are digital ID cards. The RZRA states in Section 10(1) that an ID card "in a form approved by the Director" shall be issued. RIPA states in Section 10(2) that "an appropriate identity card" shall be issued. The latter states further on, in Section 23(3)(i), that the Minister may make Regulations as to the "form and particulars to be entered on the identity cards".

Section 2 of the 2014 supplementary Regulations defines a chip as "an electronically coded-micro processing item which possesses unique biometric credentials of the authorised card holder". Section 5 of the Regulations list information to be collected for purposes of the IDs. These include a photograph, fingerprints, palms or toe prints or any "special identification mark" (for persons with disabilities such that fingerprints cannot be taken) which shall be installed in a chip. These Regulations brought in the digital aspect of the ID cards issued by the NIDA. Although NIDA ID cards contain a chip, this is not mentioned in Section 7(3)(a) and (b) which describes the content of the card. The Section states:

65 See Section 3 of the Act.

66 See Regulation 2 of the 2014 Regulations.

"(3) The card shall contain:

(a) on the face of the card:

(i) a recent photograph of the holder;

(ii) National Identity Number (NIN);

(iv) sex;

(v) expiry date;

(v) type of Identity Card;

(b) on the back side of the card:

(i) type of the Identity Card;

National Identity Number (NIN); and

(iii) issuing Authority."

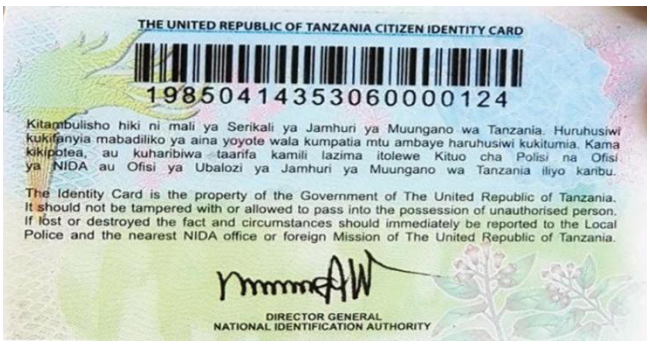

Figure 5: Specimen of the NIDA ID

(Specimen from the NIDA website (https://tanzania.eregulations.org/procedure/412?l=en))

In addition to the ID cards, both ID agencies, NIDA and ZanID, are statutory created. NIDA is established by virtue of Section 5(1) of RIPA,[67] which was reinforced by Government Notice 275A of 2011. The ZanID system is established by virtue of Section 3 of the RZRA.[68] In both laws, the registration agencies are mandated to collect biometric information[69] and issue the prescribed ID cards.

2.2 LEGITIMATE AIM

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

The law does not mention specific aims of the IDs. However, on the NIDA website, the objectives are stated as being to strengthen peace and security, the improvement of social welfare, and to boost economic development.[70]

According to a report by Gotham International, a firm that conducted the feasibility study leading to the establishment of NIDA, the system "is part of a larger vision that will further enable integration with other nationwide governmental and administration systems as well as be the starting point for secure access and usage of forthcoming eGovernment services in Tanzania".[71] Furthermore, the government has cited growing concerns about cybercrimes, reducing redundancy and duplicates within eGovernment agencies, increasing border security and control, and to ensure the delivery of quality and consistent private and public services for Tanzanians, such as student loans and opening bank accounts.[72]

Despite what is provided on the NIDA website, the Gotham International report and government pronunciations, the absence of specific aims within the law itself arguably leaves an opening for misusing information collected for purposes of registration and identification. This also means that individuals are left with little recourse in case their information is used for other unrelated or unforeseen purposes as any other purpose can be "justified" in the absence of a firm and specific legal provision as to the aims and purposes of the ID system.

67 Section 5 (1) of the Registration and Identification of Persons Act, No. 11 of 1986

68 Act No. 7 of 2015.

69 Section 9 (1) (a) of the Registration and Identification of Persons Act and 10 (2) of the Registration of Zanzibaris Residents Act.

70 *https://nida.go.tz/swahili/index.php/dhima-dira-na-maadili/*

71 Gotham International Ltd (2006), "*The Feasibility Study Report on National Identification and Registration of persons program for the Government of the United Republic of Tanzania*", at p.104/

72 Fernmelde-Union (*supra*).

A motivation for the mandatory registration and application of the ID for public and private services that is discussed less often, is the revenue generation aspect. NIDA started charging all public and private institutions that access the authority's services to serve the public.[73] According to the 2014 Regulation, every entity using NIDA information will be charged Tshs 500 (approximately USD 0,22) per click/individual. This measure saw NIDA revenues increase by 177%, from a projected Tshs 500 million to over Tshs 1.3 billion in the financial year 2019/2020.[74] This was largely due to the mandatory SIM card registration policy that was enforced for mobile users. According to the Ministry of Home Affairs (MoHA), NIDA has received approval to charge for the use of data and has been working with the office of the Attorney General (AG), under which 63 firms will sign an agreement to use NIDA data.[75]According to the Minister of Home Affairs, a total of 45 Data Sharing Agreements have been signed by NIDA with different entities between July 2020 and March 2021. In addition, NIDA is working on drafting another 22 Data Sharing Agreements from pending applications submitted to NIDA from entities requesting data sharing.[76]

2.3 DEFINING ACTORS AND PURPOSE

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

The Written Laws (Miscellaneous Amendments) Act 2019[77] named NIDA as the sole controller of data collected by NIDA.[78] Accordingly, the Act confers the power to "determine the purpose and means of use and means of processing personal data by a data recipient" to NIDA.

73 "NIDA to Start Charging Entities Using its Data", The Citizen (7/16/2020); *https://www.thecitizen.co.tz/tanzania/news/nida-to-start-charging-entities-using-its-data-2712730* accessed on 19 February 2021.

74 Peter. Felister, "Tanzania: TCRA registered 37,297,930 SIM Cards through Biometric Registration", The Guardian (19 February 2021); *https://citizenshiprightsafrica.org/tanzania-tcra-registered-37297930-sim-cards-through-biometric-registration/?lang=fr* accessed on 19 February 2021.

75 Domasa. Sylivester, "Tanzania: NIDA Projects 18m IDs in Four Months, Daily News (5/27/2020); *https://allafrica.com/stories/202005270101.html* accessed on 19 February 2021.

76 See paragraph 35 in the speech of the Minister of Home Affairs in the Parliament budgetary session 2021/2022, published on 03.05.2021. See (Only in Swahili) *https://www.moha.go.tz/sw/blog/2021-05-03/hotuba-ya-waziri-wa-mambo-ya-ndani-ya-nchi-mhe-george-boniface-simbachawene-mb* accessed on 19 June 2021.

77 No.7 of 2019.

78 Section 78 introduces a new Section 19A.

NIDA can, however, give other public and private entities licenses to access the data it holds.[79] According to the 2020 parliamentary budget speech given by the Minister of Home Affairs, such access or links to NIDA databases with other entities is given after a "Data Sharing Agreement" (DSA) has been signed between NIDA and the respective entity.[80] So far, the particulars of these Agreements have not been published. It is also not clear whether there is a "one size fits all" agreement or if the Agreements are drafted based on the specific context and entity requesting access. It is therefore also not clear whether the access to NIDA data by private entities is solely for verification purposes or also grants those entities access to the entire registry.

Currently, government agencies including law enforcement, the immigration department, civic registries, revenue authorities, student loan boards, the public recruitment secretariat, social security funds, and election commissions both in Tanzania Mainland and Zanzibar are linked to the NIDA register and can access NIDA information. According to local newspapers, these agencies have access to differential data such as ethnicity, nationality, etc.[81]

Private entities such as mobile network operators and banks also have access to information from NIDA by virtue of data sharing agreements to assist them verify customer information for service provision. This information, including sensitive personal data such as biometric information and a person's ethnicity, is shared across entities (public and private) without the knowledge and explicit consent of the data subject or a clear framework for the protection of personal data and the subject's privacy.

In addition, the ID framework itself does not provide for a redress mechanism for infringement of individual data and privacy related rights. The DSAs are not shared with the public. As such, even when these agreements provide for duties to entities recipient of personal data, a data subject is not in a position to hold the entity accountable even when their rights are violated. Data subjects are not included in the process and are unaware of neither the kind of data shared across entities nor the nature of the DSAs.

79 Section 78 of the Written Laws (Miscellaneous Amendments) Act 2019.

80 Ministry of Home Affairs, 2020.

81 Nachilongo. H, 'ID hitches mar Tanzania's election preparations', The East African Newspaper 14 Mar. 2015; Majaliwa. C, "National IDs ready in July", Tanzania Daily News 15 May 2012.

REGULATING THE PRIVATE SECTOR

The Access to Information Act of 2016 (ATIA),[82] which only applies to mainland Tanzania, allows the "public the right to access information stored under public authorities and private entities which utilise public funds and/or are in possession of information which is of significant interest to the public".[83] As NIDA is a public authority, it stands to reason that private actors can access information held by public authorities, with several exemptions as listed in the same Act under Section 6.

However, for purposes of NIDA, RIPA introduced a restriction, namely that access to NIDA information is possible upon authorisation by the Director.[84] So far, such access is granted after a data access agreement has been concluded with NIDA. Since NIDA IDs are mandatory for service provision, access by private actors is arguably inevitable as private actors would need NIDA-stored information for verification purposes. Access by private actors is subject to fees specified under the second schedule of the law.[85]

An unauthorised use of information stored by NIDA is an offence[86] with the result (upon conviction) of a punishment in the form of a fine no less than Tshs 1 million (approximately USD 440 000), and no more than Tshs 20 million (about USD 8 630), or an imprisonment sentence not less than six months but not more than two years.

In addition, the ATIA prohibits any distortion of information in the hands of a private entity. Under Section 18(1) and (2) of the Act, any actor that distorts the information they received from an information holder will be subject to an imprisonment term of not less than two years and not more than five years. Also, the Electronic and Postal Communications (SIM card Registration) Regulations oblige mobile network operators that collect biometric data to adhere to "data protection and privacy laws applicable to the situation, and any other company or business laws which may be appropriate are observed and complied [with]".[87]

Tanzania does not yet have a comprehensive data protection framework. There is a work in progress to draft a third data protection Bill after two previous

82 Act No. 9 of 2016.

83 Section 5(1).

84 Section 78. Read the inserted Section 19A(2)(b) of the Written Laws (Miscellaneous Amendments) Act 2019.

85 The Registration and Identification of Persons Act, Regulations of 2014 – Second Schedule.

86 Section 78: Read the inserted Section 19A(3) of the Written Laws (Miscellaneous Amendments) Act 2019.

87 Regulation 17(c).

efforts to draft a data protection Bill failed. The first draft Bill, which was issued in 2006, received opposition from journalists as infringing on the freedom of information. It also lacked important definitions necessary for its interpretation and enforcement. The second draft Bill was issued in 2014. A major criticism was the omission of data subject consent as a condition for the processing of personal data. The present draft has not yet been published.

DATA SPECIFICATION

Section 9 of the Act[88] lists the data to be collected in the enrolment of an individual into the digital ID system. This includes "left thumb-print or such other single finger print, and if so required by the registration officer at the time, his written signature". In addition, a person is to submit geographical data in writing. This includes their full name and surname, business and residential addresses within the United Republic, nationality, place of birth, age and sex, marital status, profession (occupation, trade, employment), and "such other particulars as the Ministry may, by an order published in the Gazette, prescribe". So far, at the time of preparation of this report, there are no orders by the Minister on additional information other than the one listed in the Act and the Regulation.

The 2014 Regulation lists additional documents to be produced, including birth certificate or evidence of birth[89] as well as birth certificate/ affidavit of birth/ evidence of birth of parents and grandparents, passport of either or both parents, primary school and Form Four leaving certificate, voter ID, and for Zanzibaris, the ZanID, driver's license and any other particulars the Minister may determine as necessary.[90]

For foreign residents and refugees, the laws require personal identity information, passport(s), birth certificate, residence permit/ refugee ID/ ration card or any other particulars that the Minister may deem necessary.[91] However, Section 9(4) exempts diplomats from recording their (or members of their family's) fingerprints.

88 Act No. 11 of 1986. See also corresponding provisions in the Registration of Zanzibaris Residents Act - Sections 7(2) and 10(2).

89 According to Regulation 5(5) of the Regulation, an evidence of birth means "a prescribed form issued by the Village/Mtaa Council to an applicant for purposes of determination and verification of his birth place, residence, identity and other matters of similar nature".

90 Cf. Regulation 5 (3) (a).

91 Cf. Regulation 5 (3) (b) of the Registration and Identification of Persons Regulation of 2014.

2.4 REDRESS MECHANISMS

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

USER NOTIFICATION

The Registration and Identification of Residents Act (RIRA) has no provision pertaining to user notifications or data breach. User notification is provided for in the ATIA, however. Under this Act, information holders are required to notify third parties of information requests they receive from interested parties.[92] Section 15(1) states:

> *An information holder dealing with a request for access to information shall take all reasonable steps to notify any third party to whom or which any record containing the information requested relates.*

The information holder (in this case NIDA) shall notify the third party (in this case data subject) within three days of receiving the request for information.[93] Apart from this, and in case of data breach, neither RIRA nor ATIA impose any obligation on the data holder or data controller to notify users or data subjects of data breaches. In addition, NIDA has no obligation under the above stated laws to ask for the consent of data subjects or to inform them whenever their data is shared or requested by any person or entity.

USER RIGHTS

ATIA gives users the right to access their information held by public authorities.[94] NIDA and private entities utilising public funds and/or that are in possession of information which is of significant interest to the public, e.g., telecommunication companies, are obliged to provide access to such information upon request.

The RIPA does not specifically provide for access rights. However, Section 22(3)(n) speaks of a fee to be paid for a "provision of extracts". This could imply that an individual has a right to request and be provided with an extract of his or her information held by NIDA. The fact that the law and its Regulations give

92 The law has neither defined "third parties" nor "interested parties". However, reading from the context of the law, third parties are the data subjects and interested parties are persons requesting access to information.

93 Section 15 (2) of the Access to information Act.

94 Section 5(1).

individuals further rights to correct information[95] implies that an individual can access, review and correct information. Once information is corrected, the law requires that the person should be issued with a new ID card with correct particulars, subject to fees charged for accessing such data as may be regulated by the Minister.[96] The costs for individuals to confirm, change information and/or renew their identity card have been specified in the revised Registrations and Identification of Persons Act of 2014.[97]

REDRESS MECHANISMS

In the enrolment process, the Act creates an administrative review mechanism in case of refusal, withdrawal or cancellation of the ID. The 2014 Regulations give an additional requirement in case of enrolment refusal, whereby a registration officer must give an applicant a written statement in a prescribed form on the grounds of his refusal.[98] An aggrieved person can appeal against actions of the registration officer to the Director of Registration.[99] If a person is still dissatisfied with the decision of the Director, they can appeal to the Minister, whose decision is final.[100] No appeal can be brought before a court.

Neither the Zanzibar nor the Tanzania Mainland laws directly address the violation of rights related to the use of IDs to access welfare. However, both laws make it an offence for a person to either tamper, unlawfully withhold, or use someone else's ID.[101] These provisions might be invoked for purposes of enforcing rights violated due to the unlawful use of the ID to access welfare or leading to the denial of welfare to the ID holder. The punishment prescribed for the above offences is a fine of up to Tshs 100 000 (approximately USD 50), or imprisonment to a prison term not exceeding one year, or both (in Zanzibar); and a fine not exceeding Tshs 30 000 (approximately USD 13) or to a prison term not exceeding three years (in Tanzania Mainland).

95 Section 13(2) and Regulation 9(1). See also Regulation 9(2) - in case of change of residence, the Regulation requires that a respective village officer – not the ID holder – to communicate the new residential information to the registrar once the ID holder introduces themselves to the local authorities for residential registration.

96 Cf. Section 22(3)(n).

97 The United Republic of Tanzania 2014.

98 Regulation 11(1).

99 Section 13.

100 The appeal to the Minister has to be made within 30 days after receipt of the statement of refusal – although an extension of time to appeal is also possible upon application to the Minister for such extension of time to appeal out of the prescribed time.

101 Section 14(1)(c)., (d) and (f) of the Registration of Zanzibaris Act and Section 20(1)(e), (g) and (h) of the Registration and Identification of Persons Act.

2.5 ACCOUNTABILITY

Are there adequate systems for accountability of governing bodies, users of Digital ID and other actors?

Section 19 of RIRA imposes a duty of non-disclosure to NIDA registration officers and immigration officers. Sub-sections (a) and (b) forbid these officers from giving access to or sharing photographs, fingerprints or personal particulars submitted for registration. The duty is further reinforced by the 2014 Regulations, which require persons enforcing this law to take an oath of confidentiality.[102] The law does not provide for any corresponding penalty in case the duty of non-disclosure is breached.

Furthermore, such access or sharing of personal data can still be allowed with written permission of the Minister in the exercise of his powers to make regulations. Under Section 19(b)(i) and(ii), the Minister may order the NIDA and immigration officers to give access to such information to third parties. The section states that no access to NIDA data shall be given to third parties, unless:

> *... with the written permission of the Minister which may – (i) refer to a person or category of persons by name, office or description; and (ii) contain such terms and conditions as the Minister may deem fit to impose.*

The law has no mechanism to ensure accountability from third parties accessing data by virtue of the above section.

To fill the regulator gap, the ATIA can be used to re-enforce accountability to both NIDA and third parties accessing and using NIDA information. Section 6(2)(e)(i) of the Act prohibits:

> *... public and private authorities in possession of a person's data from sharing the information that may involve unwarranted invasion of the privacy of an individual, other than an applicant or a person on whose behalf an application has been made.*

It also restricts access to "information that may damage the information holder's position in any actual or contemplated legal proceedings, or infringe professional privilege". Actors in contravention of this provision are liable to an imprisonment term not shorter than three years but not longer than five years.

AITA also prohibits any person from erasing, blocking, altering, concealing, and/or destroying any information held by an information holder, with the

102 Regulation 15.

intention of impeding the duties of the information holder, i.e. public disclosure of information.[103] A person convicted of such an offence will be liable to a fine not exceeding Tshs 5 million (approximately USD 2 160). or to an imprisonment not exceeding 12 months, or both.

In addition, whistleblowers receive protection against legal, administrative or employment-related sanctions under this Act.[104] This means that employees, should they report any wrongdoing or serious risks to health, safety and environment, would receive legal protection "as long as that person acted in good faith and in the reasonable belief that the information was substantially true".[105] According to the Act:[106]

> *Wrongdoing includes the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or maladministration regarding the information holder.*

In the context of the telecommunication industry, the Electronic and Postal Communications (SIM Card Registration) Regulations make it an offence for "[a]ny licensee, dealer or agent who misuses information of a customer for SIM Card registration".[107] The offence attracts a fine of no less than Tshs 5 million (approximately USD 2 160), or imprisonment for a term not less than 12 months, or to both.

Besides these examples, the Minister's power to make regulations under RIRA is extensive. While Section 22 lists several instances where the Minister may issue regulations for specific matters concerning registration and identification, Subsection 3(p) potentially opens a floodgate by giving the Minister unlimited powers to make regulations. The Minister may make such regulations on "anything which is by this Act required or permitted to be prescribed or otherwise provided for".

103 Section 22 of Act No. 6 of 2016.

104 Section 23 of Act No. 6 of 2016.

105 Section 23 of Act No. 6 of 2016.

106 Section 23(2) of Act No. 6 of 2016.

107 Regulation 20.

2.6 MISSION CREEP

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

As previously mentioned, personal data captured by NIDA are also subject to the Access to Information Act (ATIA). This means that any new services that require access to personal information are eligible by law to access the information, as long as they do not infringe on the exemption list[108] and remain within the confines of the Act.

There is also no specific regulation in place to oversee legitimacy in the processing of personal data held by NIDA. Firstly, the law does not provide for specific aims or objectives of the ID system. Secondly, the Gotham International feasibility study for the establishment of the NIDA system provides for a vague and widely stated mission for the NIDA ID system. It argues that the system is "part of a larger vision that will further enable integration with other nationwide governmental and administration systems as well as be the starting point for secure access and usage of forthcoming eGovernment services in Tanzania".[109] Thirdly, the objectives provided on the NIDA website is to ensure peace, public security as well as social and economic development. Combining all the above, NIDA is basically allowed to use information collected for whatever purpose as long as it can fit that purpose within one of the broadly formulated purposes.

108 The list on Section 6 of the Access to Information Act.

109 Gotham International, (*supra*).

RIGHTS-BASED TESTS

3.1 DATA MINIMISATION

Are there clear limitations on what data may be collected, how it may be processed and how long it is retained for, during the use of Digital ID?

RIPA does not have explicit rules on data minimisation, but Section 22 empowers the Minister to issue regulations on the methods and manner in which data is collected, published into the registers, stored, removed and destroyed.[110] The power granted to the Minister by the law to make these regulations includes decisions on the form and data to be printed on the IDs.[111] So far, based on the 2014 Regulation, information to be printed on the ID includes first names and surnames, photographs, sex, NINs, type of ID, expiration dates, and issuing authorities.[112]

However, the law seems to allow the collection of data that do not appear to be necessary for individual identification, such as the birth certificate or affidavit of birth of parents and grandparents, passports of either or both parents, primary and secondary school-leaving certificates, voter's card, driver's license, and other particulars as the Minister may determine.[113]

The law has no rules on data retention, except that the Registrar is allowed to remove invalid, false, misleading or outdated information from the register.[114] This includes information on deceased persons. To address this gap, the Records and Archives Management Act (RAMA)[115] provides for the administration and management of public records.

The Act defines a record as: [116]

110 Cf. Section 22 (3) (d) (e) (g).

111 Cf. Section 22 (3) (i).

112 Cf. Regulation 7 (3) (a) (b).

113 Regulation 5 (3) (a) of the Registration and Identification of Residents Act, Regulations of 2014.

114 Cf. Regulation 8.

115 Act No. 3 of 2020. This law applies to the Mainland and Zanzibar by virtue of its Section 3.

116 Section 2 of the Act No. 3 of 2002.

> *...recorded information regardless of form or medium created, received and maintained by any institution or individual in the pursuance of its legal obligations or in the transaction of its business and providing evidence of the performance of those, obligations or that business.*

Therefore, since NIDA is a public body keeping records as defined under this Act, its rules are applicable in this context. This Act has a "30 years rule" on data retention,[117] meaning that public authorities may retain information for 30 years before destroying it. The rule states:

> *Subject to any written law prohibiting or limiting the disclosure of information any public record, public records in the National Archives, in any other archival repository under the control of the Director or in a place of deposit appointed under section 15 of this Act, shall be available for public inspection after the expiration of a period of thirty years from their creation.*

The same Act empowers the Minister to prescribe, through regulations, longer or shorter data retention periods. Longer periods are only allowed in cases of national security, to maintain public order, safeguard revenue, or to protect individual privacy.[118] In the case of publicly accessible data, such data may be kept and be open to public access even after the expiration of 30 years.[119]

3.2 ACCESS CONTROL

The law has not established a concrete framework for access to data by private or public entities. However, by virtue of the 2021 Written Laws (Miscellaneous Amendment) Act,[120] NIDA is required to share data and create interoperability with other public institutions mandated to identify and register persons. The law specifically mentions the Registration, Insolvency and Trusteeship Agency (RITA),[121] whose Registrar is required to create an electronic register to integrate and interoperate with public registries mandated to register persons. In addition, Section 11(2)(3) seems to promote reciprocity in data sharing between public institutions mandated to identify and register persons.

117 Section 16 (1) of the Act No. 3 of 2002.

118 Section 16 (3) of the Act No. 3 of 2002.

119 Section 16 (4) of the Act No. 3 of 2002.

120 Section 11 of the Act No. 2 of 2021.

121 RITA is a public Agency managing information on persons (natural and juristic) in Tanzania. Its mandate includes registration of births, deaths, and companies, as well as safeguarding properties (including wills, deeds and trusts). insolvents

At the moment, it would seem that the NIDA database is linked to other public bodies' data registries. The Tanzania Revenue Authority, the Government Recruitment Secretariat, and the Immigration department, for example, specifically provide that once a person enters their NIDA ID details, the respective systems will "fetch" other information from the NIDA Database. Confirmation with the NIDA database will then entitle an individual access to specific services from respective entities.[122]

Otherwise, as already indicated, NIDA as a sole data controller is empowered by the law[123] to authorise other public and private entities to access certain data. In addition, Section 5(1) of ATIA grants private and public actors the right to information held by public authorities such as NIDA. Section 6(1) stipulates scenarios where the information holder is exempted from sharing information with public or private actors,[124] but the amount/level of information that an information holder can grant access to private and public actors is under the information holder's discretion – in this case NIDA – as stipulated under ATIA Section 12.

In a 2020 parliamentary report by the Controller and Auditor General (CAG) of Tanzania, it was revealed that contrary to the requirements for having memorandums of understanding (MoU) (discussed above as Data Sharing Agreements (DSAs)) between NIDA and private and public institutions before enabling access to state-held data or information, NIDA had failed to meet or enforce compliance. The CAG found that NIDA had allowed 41 private companies and 26 public institutions access to the NIDA database without MoUs (referred to as DSAs elsewhere in this document) documentation signed and in place. This means the government could not properly collect revenue or ensure safe and secure access to data by private and public institutions.[125]

122 Recruitment Manual p. 13, TRA custom licenses: *https://www.tra.go.tz/index.php/customs-licenses*

123 Section 78 of the Miscellaneous Amendment Act introducing the new Section 19A to the Registration and Identification of Residents Act.

124 Section 16(1) – The information holder may defer the provision of access to information until the happening of a particular event, including the taking of some action required by law or some administrative action or until the expiration of specified time where it is reasonable to do so in the public interest or having regards to normal or proper administrative practices.

125 PAC, Taarifa ya Kamati ya Kudumu ya Bunge ya Hesabu za Serikali (PAC) Kuhusu Taarifa za Ukaguzi za Mdhibiti na Mkaguzi Mkuu wa Hesabu za Serikali kwa Hesabu Zilizokaguliwa za Serikali Kuu na Mashirika ya Umma kwa Mwaka wa Fedha Unaoishia Tarehe 30 Juni, 2019.

3.3 EXCLUSIONS

Are there adequate mechanisms to address exclusion from the system?

The 2014 Regulations provide for the collection of alternative biometric information in case of disability that makes it impractical to collect the prescribed information, such as fingerprints, at the preregistration stage. Section 5(2) permits the use of a palm, toe prints, or any other special identification mark instead of a fingerprint when fingerprints cannot be used. In case of loss of the ID, NIDA has established a mechanism to issue a certificate which is used as a temporary ID document until the lost/damaged ID card is replaced.[126]

Section 14(1) empowers the Minister – in consultation with the relevant authority – to announce certain rights or services to only be exercised or accessed if one has the NIN. The Minister may therefore issue a regulation making it mandatory for specific services or exercise of certain civil rights to be subject to having the national ID.

This had already happened in 2019, with SIM card registration, where the Minister, by virtue of his powers to issue regulations granted by Section 11,[127] mandated the NIDA IDs as the sole ID card for purposes of SIM card registration.[128] After the Regulation, all SIM cards had to be re-registered using the NIDA IDs and be verified online through the NIDA database. Any person without a national ID could no longer register a SIM card in Tanzania – and hence cannot own a mobile phone and access mobile phone services such as communication, money transfer services, etc.

In addition, access to most public services requires a NIDA ID. This seems to be an adopted trend as it is not based on ministerial orders or regulations.[129] As long as the Minister mandates the use of NIDA IDs in a certain sector, a service provider is justified in denying an individual service in absence of a NIDA ID.[130]

126 Regulation 13

127 Of the Written Laws (Miscellaneous Amendment) Act, No. 5 of 2019. The section repealed Section 127 of the Electronic and Postal Communications Act of 2010.

128 Regulation 4 (4) of the Electronic and Postal Communications (SIM Card Registration) Regulation, 2020 States; A person shall not register any SIM Card using another person's National Identity Card except as specified in these Regulations.

129 See for example websites for the Government Recruitment Agency, Tanzania Revenue Authority, Immigration Department, before a person can access services s/he will first have to provide the NIDA ID or NIN number.

130 Section 14 (1) (2) of the Registration and Identification of Residents Act.

This potentially excludes all individuals without NIDA ID from accessing the designated "NIDA ID only" services or sectors.

Section 14(1)(2) reads:

> *(a) The Minister shall, after consultation with such authority, as may appear to him to be appropriate by regulations under this section, specify situations, services and facilities or other thing the grant or obtaining of which may be provided to depending on condition that the person identifies himself in the manner specified in section 11 of this Act*[131]
>
> *(b) Where any person…fails to do so or satisfy the authority by other proof that he is registered under this Act, the authority concerned may, notwithstanding any other written law, to the contrary, defer consideration of the application of that person until he produces either his identity card or such other proof.*

Section 11 of the RZRA provides for a corresponding provision.

Most, if not all, public institutions have moved to make the national ID or NINs a primary/ mandatory requirement for identification in order to receive services. This includes institutions like the Higher Education Loans Board, the Tax Revenue Authority, and Business Registration and Licensing Authority as well as the Government Recruitment Portal.[132] While such requirements have not been stipulated by law or regulation, clauses in relevant Acts like the Immigration Act (amended in 2015), amendment 64A, state that:

> *…the Commissioner General may, where circumstances require and within specified time, request a person to furnish to him certain documents or information for purposes of determination or verification of such person's citizenship does designate power to authorities to decide and request proof and verification of Citizenship.*

The phrase "certain documents" is at the discretion of the immigration authorities, allowing them to mandate the National ID or NINs as mandatory to access services. This provision is likely to prevent the roughly 20% of the adult population that are yet to get their NINs from being able to access social or civic services including, but not limited to, passports.

In the private sector, thus far it is only the telecom sector (through the Electronic

131 Section 11 refers to the use of NIDA IDs in identifying a person.

132 In April 2020 the director of the Public Service Recruitment Secretariat Mr. Xavier Daudi issued an order for the exclusive use of the NIDA ID in applying for public employment. See Serikali Inawataka Waombaji Wa Fursa Za Ajira Kutumia Namba Zao Za Nida (Translation: The Government requires employment seekers to use NIDA Identity numbers) at *News Update :: Public Service Recruitment Secretariat (ajira.go.tz)* accessed on 15.04.2021.

and Postal Communications (SIM Card Registration) Regulations of 2020) that has made NIDA an exclusive ID card. Registration of a SIM card cannot be completed unless the biometric data collected are verified against the NIDA database via the national IDs or NINs. Hence, the SIM card database is in effect linked to the NIDA database. If a SIM card is not registered against the NIDA ID, it is deactivated.

In February 2020, the Tanzania Communications and Regulatory Authority (TCRA) switched off roughly nine million SIM cards due to missing biometric registrations;[133] impacting both the public and private telecommunications companies. Other private actors such as the financial sector continue to accept other forms of IDs such as passports, driver's licenses, and voter IDs. However, NIDA cards would appear to be preferred as it simplifies banks' effort to verify persons through the NIDA database and reduce transactional costs such as conducting risk and cost assessments on customers and assessing the creditworthiness of borrowers.[134] However, the government intends to have NIDA IDs as exclusive IDs for provision of civic services to the citizens and residents in Tanzania.[135]

133 Odunga, 2020.

134 In the article "Tanzania Bank To Reduce Banking Costs With Use Of National ID Cards", Dr. Charles Kimei, a Managing Director of the largest Bank in Tanzania – CRDB was quoted. Read more at: *https://www.tanzaniainvest.com/finance/banking/tanzania-bank-to-use-national-id-cards-to-reduce-banking-costs*

135 The East African Newspaper, "ID hitches mar Tanzania's election preparations", 14 March 2015 at *https://www.theeastafrican.co.ke/tea/news/east-africa/id-hitches-mar-tanzania-s-election-preparations--1333560*

RISK-BASED TESTS

4.1 RISK ASSESSMENT

Are decisions regarding the legitimacy of uses, benefits of using digital ID, and their impact on individual rights informed by risk assessment?

RIRA does not provide a comprehensive framework to manage the risks associated with processing data. Other laws can also be used to support the partial framework provided by this Act in mitigating privacy and security issues, however. To ensure the correctness of data, RIRA, read with ATIA, offers a person the right to access and correct information held by NIDA (see specific provision in Section 3.1: User rights above). This would remove the risk of exclusion in case of incorrect data that does not correspond with different linked databases. Incorrect information could potentially lead to an inability to access services such as in the case of SIM card registration, or to access to financial services from financial institutions or government services such as employment and student loans, all of which are linked with the NIDA database and validated using information from NIDA.

The NIDA Registrar also has a duty to clean up data by deleting outdated and/or incorrect information from the database (see specific provisions in Section 3.2: Data minimisation above). This procedure, when properly executed, should ensure that data stored corresponds to respective individual identities to support access to the service. Additionally, the main Act makes it an offence to unlawfully deprive a person of and/or possess another person's ID cards or use an ID card issued to another person.[136] It is also an offence for a person to give another person their ID card to access services or to falsify an ID card and use it to access services.[137] These offences are punishable with a fine not exceeding Tshs 30 000 (approximately USD 13), or a prison term not exceeding three years, or both.[138]

The Cybercrimes Act[139] comes into play to mitigate unauthorised access and

136 Section 20(g) and (h) of the Act No. 11 of 1986.

137 Section 20(i) and (k) of the Act No. 11 of 1986.

138 Similar offences have been created by the Registration of Zanzibaris Residents Act under Section 14(1)(c), (d), (f), (h) and (i). The punishment is a fine of no less than o Tshs 100 000 (approximately USD 44) or imprisonment not exceeding one year or both.

139 Act. No of 2015

data breaches. The Act penalises illegal access, use, destruction or interference with functioning, usage or operation of computer systems and computerised data.[140] It is also an offence to intercept computer systems or circumvent protective measures implemented in a computer system to prevent access to non-public data,[141] or to interfere with the functioning, usage or operation of a computer system.[142] In addition, the Act creates an offence for data espionage.[143]

To protect the database, the Minister is empowered under Section 28 of the Cybercrimes Act to make regulations and designate a computer system as critical information infrastructure. Once such a regulation is published, special guidelines and procedures in the access, use and management of such information infrastructure are prescribed. These would include the: [144]

> *... transfer and control of data, integrity and authenticity of data or information contained in any critical information infrastructure, methods to be used in the storage or archiving data or information, disaster recovery plans in the event of loss of the critical information infrastructure or any part of critical information infrastructure and manner and procedure for carrying out audit and inspection.*

As far as could be ascertained, the NIDA system has not been designated as a critical information infrastructure by Ministerial Order or regulation.

In the context of SIM card registration, when a national ID has been used in

140 Under Sections 4, 5, 7 the liability for unauthorised deletion, modification, blocking/ destruction of data, disclosing / sharing of data or access code / program to facilitate an unauthorised access to or even receiving unauthorised computer data ranges from a fine of one to Tshs 10 million (approximately USD 4 400) – or three times the value of undue advantage received whichever is greater or an imprisonment term ranging from one year to three years or both fine and imprisonment. In addition, Section 11 imposes a minimum fine of Tshs 20 million (approximately USD 8 800) for unlawfully altering computer data.

141 Section 6. This offence is punishable by a fine of not less than Tshs 5 million (approximately USD 2 200) or to imprisonment of not less than one year or to both.

142 In Section 9, a punishment for interference with the functioning of computer system is to a fine of not less than Tshs 2 million (approximately USD 870) or three times of value the undue advantage received, whichever is greater, or to imprisonment for a term of not less than one year or to both. See also Section 12 on computer fraud.

143 The Act has not defined data espionage, but Section 8 would suggest data espionage to be when a person "obtains computer data protected against unauthorised access without permission". Punishment for data espionage is a fine of not less than Tshs 20 million (approximately USD 8 800) or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than five years or to both. See Section 8 of the Act.

144 Section 28(2)(a-h) of the Cybercrimes Act, No. 4 of 2015. The punishment for interference with critical information infrastructure is prescribed under Section 29 as a fine not less than Tshs 100 million(approximately USD 44 000) or three times the loss occasioned or to imprisonment for a term not less than five years or to both".

fraudulent activities (e.g., stolen identity to commit fraud), then the Electronic and Postal Communications (SIM Card Registration) Regulation mandates NIDA to flag the identity for 90 days to prevent further fraudulent activities.[145] The Regulation places the burden on telecommunication providers to identify any national IDs involved in fraudulent activities across its network and immediately notify NIDA.[146] Furthermore, the service providers are to "compensate a victim of any material loss suffered from fraudulent activity associated with biometric SIM Card registration of which the service provider failed to identify the responsible customers".[147]

4.2 PRIVACY RISK MITIGATION

As noted, Tanzania has no data protection law, although two draft Bills, the 2006 Freedom of Information Draft Bill and the 2014 Draft Data Protection Bill,[148] have been published in the past. Currently, there is a third Data Protection draft Bill, but it has not yet been published. The 2006 draft Bill did not pass due to criticisms that it curtailed freedom of information to journalists. The 2014 draft Bill also received criticism, including for omitting individual consent as a condition for processing personal data.

Privacy is broadly protected under Article 16 of Tanzania's Constitution,[149] subject to the usual limitations in the exercise of individual rights. However, the constitutional right to privacy is further limited in a sense that it lacks specific substantive and procedural mechanisms to enforce it. For example, the Constitution does not provide for specific rights and corresponding duties that are usually found in data protection laws. This means, data protection principles and risk mitigation mechanisms found in data protection laws such as privacy-by-design and privacy-by-default are not available (at least legally not provided for) in Tanzania.

Risk mitigation mechanisms in data protection laws serve to reinforce accountability for data controllers, as they require data controllers to be proactive

145 Regulation 17(f).

146 Regulation 17(e).

147 Regulation 17 (d).

148 As mentioned in Section 3.1 above on *regulating the private sector*, the 2006 draft Bill did not pass due to criticisms that curtailed freedom of information to journalists. The 2014 draft Bill also received criticisms including for omitting individual consent as a condition for processing personal data.

149 The Article states, "[e]very person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications".

(as opposed to being reactive) in protecting individual privacy and personal data. Through mechanisms such as privacy-by-design and privacy-by-default,[150] privacy and data protection become the first consideration before any data processing activity takes place. Taking a proactive approach would, for example, require ID systems to integrate data privacy needs and security measures before any processing of personal data can take place. This includes making data protection impact assessments to assess potential risks involved in processing certain types of data and putting in place appropriate security measures (encryption or data anonymisation) vis-a-vis potential security risks. It would also require the controller to determine the necessity, accuracy and sufficiency of data in specific contexts. The absence of a data protection law or regulatory framework in Tanzania to enforce these standards creates a potential privacy risk to personal information processed by NIDA.

Regulation governing the collection and protection of personal data exists only in the context of telecom and postal activities by virtue of the Electronic and Postal Communications (Consumer Protection) Regulations of 2018. These Regulations establish rules and conditions for processing personal data. Regulation 6(2) mandates authorities collecting and processing personal information to do so fairly and lawfully, for identified purposes, and in accordance with consumers' other rights. The Regulations also impose a duty to authorities to ensure that data is accurate and protected against unauthorised or accidental disclosure or transferred to third parties without data subjects' consent or legal basis.

So far, there is no law or regulation that differentiates between ordinary and sensitive personal data. The only regulation that currently differentiates information categories, is the Bank of Tanzania (Credit Reference Bureau) Regulations, which contains a category of "prohibited information" (including information about "race, creed, colour, ancestry, ethnic origin, religious or political affiliation, state of health or criminal record except financial fraud and other similar types of offences...information on individual judgment, bankruptcy or liquidation").[151] Credit institutions are prohibited from maintaining such information in their databases or including them in their credit reports.

150 Privacy by design is people-centric and it involves training and cultivating privacy and data protection culture within the organisation. Privacy by design is technical-centric and involves the use of technology to protect and secure personal privacy and data.

151 Regulation 20(1)(2) of the Bank of Tanzania (Credit Reference Bureau) Regulations, No. 416 of 2012.

4.3 RESPONSE TO RISK

Does the governance regime provide strategies for dealing with risks, once they arise?

The NIDA database is housed in a data centre which conforms to recognised international standards of ISO 27001 and ISO 9001.[152] These global standards require data holders to ensure their data centres are regularly audited for information security risks, taking account of potential threats, vulnerabilities, and impacts. This includes designing and implementing a robust system of information controls to mitigate and address risks associated with data handling, transfer, and consumption. Other than that, there appears to be no known or published measures to reduce risk of exclusion to social services based on either system failure in general or failure in the authentication of the ID system and power cuts.

In case of emergencies such as power cuts or system failures, the data centre is equipped with a disaster recovery site. This is a mirror site that can be used to operate the national ID system in case of emergencies.[153]

152 Fernmelde-Union, (*supra*).

153 *Ibid*, p. 53.

CONCLUSION

Since independence in 1961, Tanzania has had a vision to provide her citizens with legal identity. This signals that Tanzania recognises the need for her citizens to be able to identify themselves and access civic services. Although this vision took more than 50 years to materialise, Tanzania managed to establish a digital ID system, registered 22 million Tanzanians and issued a unique identifier number to every single registered person, a number that will be used to identify this person for the rest of their life. Through this number, a person can be able to access online and offline services. Despite this achievement, there are critical issues with the ID system in Tanzania.

1. Accountability and transparency: There is neither an accountability mechanism nor transparency in the way the system operates, especially in relation to the use of personal data. The non-disclosure duty under the Registration and Identification of Citizens Act prohibits NIDA officers from disclosing personal information collected in the identification process. The provision has no corresponding penalty or means to hold an officer accountable in case an officer breaches that duty.
2. Furthermore, NIDA as the sole data controller is entrusted with a lot of personal and very sensitive data – including biometric data of citizens of Tanzania. The law allows NIDA to enter into data sharing contracts with private and public entities but it does not provide for a transparency mechanism. So far, 45 Data Sharing Agreements have been concluded. However, neither NIDA nor the responsible Minister has made public the nature of these agreements. It is not publicly known what kind of data is shared, for what purpose and for how long. Citizens are not informed on how their personal information is being used by NIDA and other organisations. In other words, citizens are not in a position to enforce their privacy rights since they are unaware of the nature of processing and sharing activities by NIDA. Citizens are also unaware of the identity of other entities with access to their personal data.
3. Data/ privacy protection framework: Tanzania is yet to enact a comprehensive data protection law. So far, the laws governing registration and identification of citizens, communication and cybersecurity laws combined fail to give sufficient protection to personal data and privacy in the context of the digital ID. The constitutional right to privacy is limited and insufficient in this context. It lacks clear rules (on rights and obligations) and procedural

mechanisms for its enforcement. There is a need for a data protection framework that creates rights, duties and a clear enforcement mechanism. Data protection laws, in addition to providing rights, duties and redress mechanisms, would normally establish data protection authority. Data protection authority will have the mandate to enforce the law to all entities (public and private) processing personal data, including NIDA, and therefore, increase accountability in the ID system.

4. Exclusion risks: According to ministerial declarations, Tanzania has a long-term goal of making the NIDA IDs exclusive identity cards. If this goal is executed as planned, there is the potential to exclude individual access to basic social services. To avoid such risk, Tanzania would need to make an "exclusion risk assessment" before implementing such a measure. There are technological, social and literacy gaps (to mention just a few) that may make access to NIDA IDs difficult. The idea should be to increase "legal identity" to support access to services rather than to have "NIDA ID" as an impediment to access services. Ideally, the ID system should be interoperable with other functional ID systems in place, allowing people to access services – pending issuance of the NIDA ID or in case of (NIDA) authentication failure.

SPECIFIC RECOMMENDATIONS

THE GOVERNMENT OF TANZANIA

The government should consider improving the law on identification and registration of citizens in the following aspects:

Accountability, transparency and data (privacy) protection: there is a need for the MoHA and NIDA to be transparent on the DSAs. A citizen of Tanzania has the constitutional right to privacy which includes "security of his person" (Article 16(2)). To enforce this right and "secure his person" a citizen must be informed of activities involving his personal data and that are potentially harmful to his privacy and security of his person. Eventually, the Ministry of Home Affairs MoHA) and NIDA have a constitutional duty to open to the public the DSAs to give individuals an opportunity to satisfy themselves on the protection of their privacy and personal data security in these transactions. I therefore recommend:

Firstly, that RIRA be reviewed/amended to provide for a clear and transparent framework for data sharing agreements between NIDA and other entities. At the minimal level, the law should be clear on the basic conditions (rights and duties) and scope of a DSA. The law should also provide for a mandatory publication of these agreements and allow public access / consultation before they are signed. This should go along with a possibility of individual "opting out" of the bulky data sharing with specific entities.

Secondly, the government should create a robust security and protection framework. RIRA was adopted in 1986; it does not reflect the current technological advancement in the context of the digital IDs. In fact, the ID envisioned in the Act is a "simple" paper-based ID not involving biometric data or online authentication procedure. The review/amendment of the law is inevitable in addressing possible security issues based on the technology used for the IDs. This goes along with developing a framework for the protection of personal data and privacy. With regards to the protection framework, as already mentioned in the conclusion, Tanzania needs to improve its privacy and data protection legal framework.

There are reportedly ongoing efforts to draft a data protection bill. This is a positive development. However, a few things need to be considered. The UN Human Rights Committee (UNHRC) has recently issued a pronouncement on Mauritius with regards to protection of personal data and privacy in the context of digital IDs. The pronunciation is an indication that having a data protection framework does not *prima facie* guarantee or secure individual privacy on data stored on identity cards. This is because Mauritius has a comprehensive data protection law but the UNHRC still found its ID system to be insecure. In the context of digital IDs, the protection framework has to factor in the nature of technology deployed and sensitivity of data collected (such as biometric data) which might require a specific or more robust protection framework than that provided by data protection laws. As an example, the pronunciation by the UNHRC mentioned above, it was discovered that the radio frequency identification technology (RFID) used to store biometric data in the IDs could be copied without physical contact of the card or knowledge of the card holder, using RFID readers which are easily bought online. This information could be copied onto a falsified card. Security and protection frameworks need to pay attention to specific ID systems and/or infrastructure, the technology used as well as the type of data stored in order to develop appropriate legal, regulatory and security measures. These measures can be created separately from and in addition to a data protection framework to address specific vulnerabilities in the ID system. To have such a protective system, I would recommend that the Tanzanian Government considers a holistic approach that involves policy makers, legislators and technologists working together to create a suitable security framework for the ID system and protection framework for individual ID holders.

In addition, an important aspect in any protection framework is an effective redress mechanism. In this context, it is important for the framework to consider having a data breach notification. This is an important aspect in protecting and securing personal privacy and data. Data breach notifications serve two purposes; firstly, they create a duty to data controllers/processors. Breach notification would normally require a data controller/processor to notify data subjects and other affected parties of data breaches, which includes unauthorised access to

personal data. This also gives the data controller/processor an opportunity to assess security measures in place and implement proper remedial measures. Secondly, notifications enable individuals to be proactive in protecting their data and privacy. For example, if a data/security breach relates to an individual bank account, a notification will help account holders to take countermeasures such as changing a password to mitigate the effects of the breach and secure their account and finances.

NIDA ID exclusivity: Making NIDA IDs exclusive has the potential to exclude citizens from civic services. This can happen not only because an individual has no NIDA ID or NIN, it can also happen due to failure in the authentication process. In this light, I would recommend the Government of Tanzania allow for a parallel use of NIDA IDs with other functional IDs such as voter ID, driver's licenses etc. In which case, the system should allow individuals to opt out of the NIDA ID and opt in to other functional IDs to access specific services such as SIM card registration, public employment or student loans.

TECHNOLOGISTS

Technologists have an important role in building up and managing ID systems. My recommendation is for technologists to work beyond construction and management of ID systems and consider cooperating with the government, policy makers and legislators to secure ID systems. Technologists have the technical know-how of the ID systems and are best placed to advise on the proper security measures as well as policy and legislative considerations for a secure digital ID system.

CIVIL SOCIETY

Civil society and human rights organisations have an important role in creating public awareness on the importance and implications of digital IDs. Civil society and human rights organisations could assist the government to bring public awareness of the opportunities that can be realised through universally safe and secure digital identification in Tanzania.

For further research

As far as this research is concerned, no evidence could be found on any research conducted by the government in Tanzania to determine potential exclusion of the marginalised before the NIDA system was deployed. I believe there is still a need to evaluate areas or populations that are susceptible to exclusion because of geographical position, illiteracy, gender, age, civic status or the ID system and its associated technology.

REFERENCES

"NIDA to Start Charging Entities Using its Data", The Citizen (16 July2020); *https://www.thecitizen.co.tz/tanzania/news/nida-to-start-charging-entities-using-its-data-2712730* accessed 19 February 2021.

"Rush for IDs in Zanzibar", The New Humanitarian (3 April2006) *https://www.thenewhumanitarian.org/report/58639/tanzania-rush-ids-zanzibar* accessed on 23 February 2021.

"Tanzania: PM: Tight ID Card Filing in Border Regions Right", *https://citizenshiprightsafrica.org/tanzania-pm-tight-id-card-filing-in-border-regions-right/* accessed on 19 February 2021.

Burt. C, "Tanzania Leverages Increased Knowledge and Skill to Move toward Universal Biometric Identity" in *BiometricUpdate.com*, 2018, *https://www.biometricupdate.com/201805/tanzania-leverages-increased-knowledge-and-skill-to-move-toward-universal-biometric-identity* accessed on 22 February 2021.

Domasa. Sylivester, 'Tanzania: NIDA Projects 18m IDs in Four Months, Daily News 27 May 2020); *https://allafrica.com/stories/202005270101.html* accessed on 19 February 2021.

Fernmelde-Union, Internationale. "Digital identity roadmap guide", Geneva: International Telecommunication Union, 2018.

Fewer Africa, "Electoral Violence and Reconciliation Zanzibar", Nairobi, 2008; *https://reliefweb.int/sites/reliefweb.int/files/resources/E3DB1AAD353D4D3649257046001A4BC7-fewer-tza-20jul.pdf* accessed on 23 February2021.

Gotham International Ltd, "The Feasibility Study Report on National Identification and Registration of persons program for the Government of the United Republic of Tanzania", 2006.

Global Voices Advox, "Deadline looms for biometric SIM card registration in Tanzania", 22 January2020; *https://advox.globalvoices.org/2020/01/08/deadline-looms-for-biometric-sim-card-registration-in-tanzania/* accessed on 22 February2021.

Yusuf. Issa, "Zanzibar demands more from NIDA", HabariLeo (3/8/2021); *https://habarileo.co.tz/habari/zanzibar-demands-more-from-nida.aspx* accessed on 8 March 2021.

ID4Africa, "Identity for All in Africa", (2/22/2021); *https://id4africa.com/* accessed on 22 February 2021.

Makoye. Kizito, "Tanzania Launches New ID Cards to Combat Election Fraud", Thomas Reuters (2/22/2021); *https://news.trust.org/item/20130227092500-jm6av/* accessed on 2/22/2021.

Ministry of Home Affairs, Parliamentary Budget Speech of 2020/21. Dodoma, Tanzania: The Tanzania Parliament, 2020.

Mhagama. Hilda, "Tanzania: Public Warned against Unregistered SIM Cards", Daily News (29 July 2013); *https://allafrica.com/stories/201307291551.html* accessed on 22 February 2021.

Mwangonge. Henry, "Tanzania Begins Biometric Registration of Mobile Users", The Guardian (22 February 2021); *https://www.ippmedia.com/en/news/tanzania-begins-biometric-registration-mobile-users* accessed on 22 February 2021.

Nagai. Melamari Simon, "The Challenges and Need of Legal Frameworks for Data Protection in Tanzania: Case Study of Tanzania National Identification Authority (NIDA)", Master's Dissertation, Open University of Tanzania, Dar es Salaam. *http://repository.out.ac.tz/1061/1/Nagai_Melamali.pdf* accessed on 22 February2021.

Odunga, Maureen, "Tanzania: Three Million Switched Off SIM Cards Now Retrieved", Tanzania Daily News (16 March 2020). *https://allafrica.com/stories/202003160632.html*, updated on 16 March 2020, accessed on 9 June 2021.

PAC, Taarifa ya Kamati ya Kudumu ya Bunge ya Hesabu za Serikali (PAC) Kuhusu Taarifa za Ukaguzi za Mdhibiti na Mkaguzi Mkuu wa Hesabu za Serikali kwa Hesabu Zilizokaguliwa za Serikali Kuu na Mashirika ya Umma kwa Mwaka wa Fedha Unaoishia Tarehe 30 Juni, 2019.

Peter. Felister, "Tanzania: Kids Lined up for NIDA Numbers". The Guardian (19 February 2021); *https://citizenshiprightsafrica.org/tanzania-kids-lined-up-for-nida-numbers/* accessed on 19 February 2021.

Peter. Felister, "Tanzania: TCRA registered 37,297,930 SIM Cards through Biometric Registration", *The Guardian* (19 February 2021); *https://citizenshiprightsafrica.org/tanzania-tcra-registered-37297930-sim-cards-through-biometric-registration/?lang=fr* accessed on 19 February2021.

Sanga, Christopher, et al, Decentralization of birth registration to Local Government in Tanzania: the association with completeness of birth registration and certification. In *Global health action* 13 (1), (2020). DOI: 10.1080/16549716.2020.1831795

United Nations Office for Partnerships, "ID2020 Summit 2016" *https://www.un.org/partnerships/news/id2020-summit-2016* accessed on 19 February 2021.

UNPO, " Zanzibar: All Adults Must Carry Identity Cards by 1 April", *https://unpo.org/article/3884* accessed on 23 February 2021.

WEF, "A Billion People have no Legal Identity - But a New App Plans to Change That", World Economic Forum (22 February 2021); *https://www.weforum.org/agenda/2020/11/legal-identity-id-app-aid-tech/* accessed on 22 February 2021.

The World Bank, "The State of Identification Systems in Africa", *https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-*

country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y accessed on 22 February 2021.

The World Bank, "Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey", Washington, DC. *http://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf* accessed on 22 February 2021.

Zanzibar Civil Status Registration Agency (ZCSRA), "Wazanzibari Sasa Kutambuliwa Kidigitali (E-ID Card)", *https://www.zcsra.go.tz/resources/view/wazanzibari-sasa-kutambuliwa-kidigitali-e-id-card* accessed on 8 March 2021.

The Laws

The Access to Information Act, No. 9 of 2016.

The Bank Of Tanzania (Credit Reference Bureau) Regulations, GN. No. 416 of 2012.

The Constitution of The United Republic of Tanzania, 1977 (As amended from time to time).

The Cybercrimes Act, No. 4 of 2015.

The eGoverment Act, No. 2 of 2019.

The Electronic and Postal Communications (Computer Emergency Response Team) Regulations, GN. No. 60 of 2018.

The Electronic and Postal Communications (Consumer Protection) Regulations, GN. No 61 of 2018.

The Electronic and Postal Communications (Online Content) Regulations, GN. No 538 of 2020.

The Electronic and Postal Communications (SIM Card Registration) Regulations.

The Electronic and Postal Communications (SIM Card Registration) Regulations, GN. No. 112 of 2020.

The Electronic and Postal Communications Act, No. 3 of 2010.

The Immigration (Amendment) Act, No. 8 of 2015.

The Records and Archives Management Act, No. 3 of 2002.

The Registration and Identification of Persons Act, No.11 of 1986.

The Registration of Zanzibaris Act, No. 7 of 2005.

The Registrations and Identifications of Persons (General) Regulations, 2014.

The Tanzania Citizenship Act, No. 6 of 1995.

The Written Laws (Miscellaneous Amendments) (No. 2) Act, No. 4 of 2021.

The Written Laws (Miscellaneous Amendments) (No. 5) Act, No. 2B of 2019.

The Written Laws (Miscellaneous Amendments) Act, No. 7 of 2019.

The Written Laws (Miscellaneous Amendments) Act, No. 4 of 2003.

The Zanzibari Act, No. 5 of 1985.

ANNEX 1

OVERVIEW OF EVALUATION FRAMEWORK

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

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

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

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

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

RULE OF LAW TESTS

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

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

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

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

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

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

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

RIGHTS-BASED TESTS

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

These tests ask five questions about:

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

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

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

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

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

RISK-BASED TESTS

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

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

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

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

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

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

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