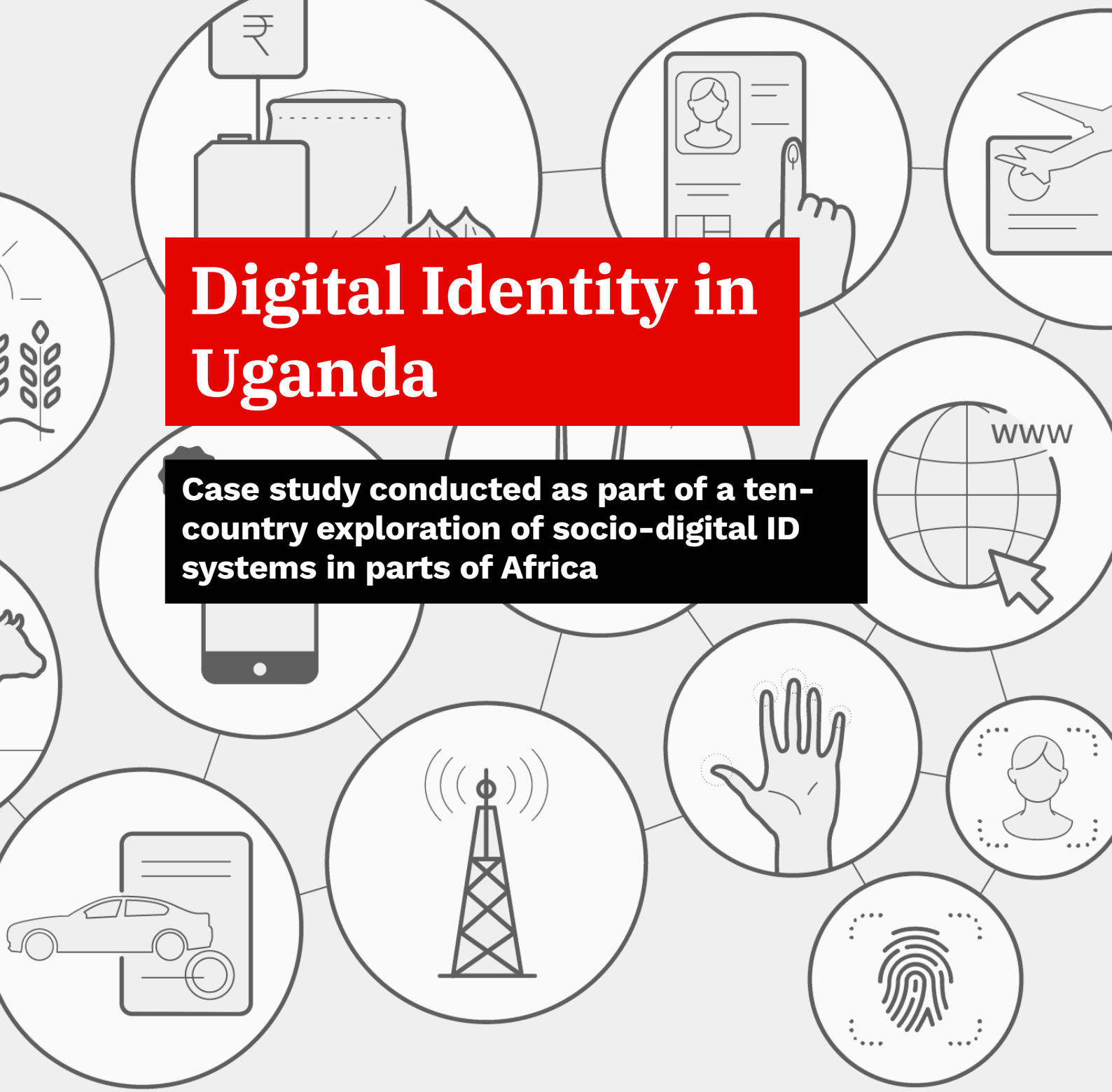


Digital Identity in Uganda

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

RESEARCH & WRITING
Neema Iyer

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 Uganda

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 Uganda

By Neema Iyer, Pollicy Uganda

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 Ugandan case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Neema Iyer. 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 Neema Iyer, 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 focus of this report is the Ugandan national digital ID project. As governments all over the world attempt to promote the establishment of legal identity systems to promote better planning for welfare and service delivery, it is important to evaluate the impact of these efforts on human rights, democracy, privacy and their economy.

In the course of preparing this report, we evaluated the legitimate purpose behind Uganda's national digital identity programme and the legal and administrative systems put in place to oversee it. The programme is administered primarily by the National Identification and Registration Authority, which was set up under the Registration of Persons Act in 2015 to promote the Ugandan government's plan to improve security and welfare planning and delivery. The scheme is also, to a lesser extent, regulated by National Information Technology Authority Uganda, under the auspices of the Data Protection and Privacy Act of 2019.

Some of the issues evaluated in the report include the over-collection of personal data as part of the registration process and the inadequacy of the current data protection safeguards. Our report also revealed that there is a high potential for mission creep in the set-up of the system, evidenced by the government's decision to share the collected data with members of the police force and private telecommunications businesses. Also of note is the alarming prevalence of exclusionary practices against societal minorities such as women, the elderly and the economically disadvantaged. It is hoped that this evaluation of and recommendations for Uganda's national ID system would be useful to the Ugandan government and will guide and provide insight for future policy deliberations.

ACRONYMS AND ABBREVIATIONS

AID	Alien Identification Card
DCIC	Directorate of Citizenship and Immigration Control
DPP	Director of Public Prosecutions
DPPA	Data Protection and Privacy Act
GISO	Gombolola Internal Security Officer
ID	Identity
LC	Local Council
MoIA	Ministry of Internal Affairs
MoFPED	Ministry of Finance, Planning and Economic Development
NIN	National Identification Number
NIRA	National Identification and Registration Authority
NSIS	National Security Information System
OPM	Office of the Prime Minister
ROPA	Registration of Persons Act
SAGE	Social Assistance Grants for Empowerment
SCG	Senior Citizens Grant
UGX	Ugandan Shilling
URSB	Uganda Registration Services Bureau

CONTENTS

INTRODUCTION

Uganda's current population is estimated at 39 million, with an annual approximate growth of 3% a year. Uganda is one of the most diverse countries in the world, with 41 living languages spoken in the country and over 54 ethnic groups, in addition to significant numbers of Arabs, Asians, and Europeans, within the borders. The current President of Uganda is Yoweri Kaguta Museveni, who came to power in 1986 after a six-year guerrilla war. Following constitutional amendments removing term limits on the President, he has been President of the country for the past 35 years. The cultural history of Uganda has resulted in visible complex cultural-regional loyalties and interactions between traditional kingdoms, religions and centres of power today. This cultural diversity and the country's political history of authoritarian democracy are of particular importance to the development of a unifying identity system in the country.

According to the 2012 Report of the Committee on Defence and Internal Affairs on the Inquiry into the Procurement of Equipment for the National Security Information System Project (NSIS)/the National ID Project,[9] as far back as 2004, several initiatives designed to create a database of information and identification had been designed by various parastatal organisations. According to the report:

> *The idea of the national data bank picked [up] momentum in 2004, when the [Ministry of Internal Affairs], under Minute No. 34 (CT 2004) Cabinet approved the setting up by [the] Government of a National Bio-Data Bank in the Ministry of Internal Affairs for easy access by the Government Institutions. Subsequently, the President, on 3rd April 2009, appointed the 3rd Deputy Prime Minister and Minister of Internal Affairs to coordinate inter-ministerial efforts in the execution of the project. Around the same period 2004-2009, the [Ministry of Finance, Planning and Economic Development] was working on a similar project, named the National Population Data Bank. On 2nd April 2008, under Minute 155 (CT 2008) Cabinet adopted a Standing Committee chaired by the Third Deputy Prime Minister and Minister of Internal Affairs (3rd Dep. PM/MoIA) to provide political leadership in the revamping efforts to set up the information system. This information system has also been variously referred to by different institutions, such as the National Identity Card Project, the Uganda Population Data Base, Identification and Verification Project, and the National Security Documentation Project. Currently, the project is known as the National Security Information System....*

9 Committee on Defence and Internal Affairs, *Report of the Committee on Defence and Internal Affairs on the Inquiry into the Procurement of Equipment for the National Security Information System Project (NSIS)/ the National ID Project* (Kampala: Parliament of Uganda, 2012), 3, accessed 26 July, 2021, *https://www.parliament.go.ug/cmis/browser?id=7c240510-4fe3-4f58-9758-d1b6e06876fe%3B1.0.*

In 2014, the Government of Uganda launched the national ID programme under the National Security Information System (NSIS) project to reform civil registration and identification ahead of the 2016 elections.[10]

Subsequently, the NSIS project was converted into a permanent national foundational digital ID, defined by the World Bank to mean identity systems "which are built in a top-down manner with the objective of bolstering national development by creating a general-purpose identification for use across sectors"[11] system leading to the enactment of the Registration of Persons Act (ROPA) of 2015.[12] Consequently, the ROPA repealed the previous Births and Deaths Registration Act[13] and transferred the registration of births and deaths function from the Uganda Registration Services Bureau (URSB) to the National Identification and Registration Authority (NIRA). The Authority was established under Section 4 of the ROPA to be responsible for bringing both civil registration and national IDs under one organisation.

However, many Ugandans have been unable to acquire national IDs. In 2019,[14] it was reported that at least 2.4 million Ugandans (about 6% of the population) aged 16 and above had not enrolled for national identity cards. The figure includes 585,265 people whose applications for national IDs were unsuccessful because they provided insufficient and inconsistent information, or had gaps in their documentation. This may be due to a lack of documents such as a birth certificate (in the case of home or rural births), a marriage certificate (in the case of traditional weddings), etc.

According to NIRA,[15] between 2013 when the exercise commenced and 2019, a total of 17 558 052 national IDs had been physically printed for distribution to citizens, accounting for 74.05% of the 23 710 691 Ugandans who have been allocated National Identification Numbers (NINs) by NIRA. Essentially, while the

10 Committee on Defence and Internal Affairs, *Report of the Committee on Defence and Internal Affairs on the Inquiry into the Procurement of Equipment for the National Security Information System Project (NSIS)/ the National ID Project*, 5.

11 World Bank Group, Digital Identity Toolkit: A Guide For Stakeholders In Africa (Washington DC: World Bank Group, 2014), 4, accessed 26 July 2021, *https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y.*

12 The Registration Of Persons Act, No. 4 of 2015. *https://www.ict.go.ug/wp-content/uploads/2018/06/Registration-of-Person-Act-2015.pdf*

13 Births and Deaths Registration Act, CAP 309 of 1973. *https://www.parliament.go.ug/cmis/browser?id=ed282ea6-3b20-460e-85bd-1c64ac6db0d9%3B1.0.*

14 "2.4 million Ugandans don't have national IDs," *Daily Monitor*, February 6, 2019, *https://www.monitor.co.ug/News/National/2-4-million-Ugandans-don-t-have-national-IDs/688334-4970294-ohwoha/index.html.*

15 *Ibid.*

majority of Uganda's 23.7 million citizens (about 58% of the 40.3 million reported population in 2019) have been allocated NINs and have received a physical ID card, many others are yet to do so. This is problematic, because for many services, such as SIM card registration, a physical ID must be presented. A photocopy of the ID, physical passport or other IDs, or just the NIN is not acceptable proof of identity.[16]

This significant gap in the acquisition of legal identification means that millions of Ugandans are unable to access basic services including the opening of bank accounts, selling or purchasing land, taking out loans, obtaining passports and even getting jobs. In addition, the foundational nature of the national digital ID project in Uganda is such that all civil registration and identity verification activities, including voter registration, are impossible without a national ID.[17] For example, in March 2017, Uganda Communications Commission's (UCC) Executive Director, Godfrey Mutabazi, directed all telecom operators in the country to verify SIM cards against the NIN (or passports for foreigners) for all subscribers.[18] To put this in context, if a citizen loses their wallet and phone, they would have to engage with a months-long ID replacement process before they can obtain a new SIM card for their phone. Again, a photocopy, scan or just the NIN will not suffice - an original, physical ID is required.[19]

Despite the promises made about using digital verification and integration in Uganda's ID project, with such trappings as biometric and face capturing, and the generation of NINs, the ID project has yet to abandon the old methods of documentation and registration fully. This is because data integration and processing are carried out at the headquarters in Kololo, a suburb of the capital city Kampala, after receiving it from district offices that physically send all written

16 Uganda Communications Commission, The Uganda Communications Commission Operational Guidelines On Sim Card Registration In Uganda (Kampala: Uganda Communications Commission, 2020), 3 - 4, accessed 20 August 2021, *https://www.ucc.co.ug/wp-content/uploads/2020/12/All-Telecoms.Operational-Guidelines-on-simcard-registration..pdf.*

17 Gilbert Habaasa and Jonan Natamba, "Civil registration and national identity system all under one roof: Uganda's fastest path to the revitalization of CRVS for Africa," Statistical Journal of the IAOS 34 (2018): 456-57, *https://doi.org/10.3233/SJI-180429.*

18 "Ugandan Telecoms to Deactivate all Unregistered SIM-cards Tonight," The Independent, 29 March 2017, *https://www.independent.co.ug/ugandan-telecoms-deactivate-unregistered-sim-cards-tonight/.*

19 Uganda Communications Commission, The Uganda Communications Commission Operational Guidelines On Sim Card Registration In Uganda 3 - 4.

and digitally stored applications.[20]

According to the 2018 report by the Office of the Auditor-General:

> *The delays at the transmission of data from the field offices to the processing [centre were] attributed to the fact that there was no online system for transmission of information from the points of registration (district offices) to Kololo where data processing is done. Enrolment data is transmitted using external storage devices by NIRA staff from the field offices to Kololo. This implies that transmission of enrolment data is not real time. In some cases, especially up country field offices, data is delivered only two or three times a month.*[21]

This has led to the observation that the Ugandan national digital ID scheme "is a system that may be digital at its core but is still mostly analog on the periphery".[22]

It is the reasoning of the authors that an ID should not be a crucial tool to receiving public services. It will later be explained how ID systems, especially those formulated on systems drawn from foreign contexts and implemented without public consultation or civil society input, can be exclusionary and cause more harm than good. These systems can also be also another tool in an authoritarian government's toolbox to surveil and oppress citizens, and particularly, dissenting voices.

This introduction has provided an overview of the past and current efforts to develop a national identity programme by the Ugandan government. The rest of the report will contain further analysis and assessment of the programme and its impact, following the CIS evaluation framework.

METHODOLOGY

This report was compiled using primarily desk-based research that relied on reports, newspaper articles and journal articles by various local and international

20 Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done? (Kampala: Unwanted Witness, 2020), 8, accessed 19 May 2021, *https://www.unwantedwitness.org/download/uploads/Ugandas-Digital-Identification-Systems-and-Processes-in-a-protracted-crisis.pdf.*

21 Office of the Auditor-General, A Value For Money Audit Report on the identification and registration of persons by the National Identification and Registration Authority (NIRA) (Kampala: The Republic of Uganda, 2018), 16, accessed 29 July, 2021, *http://www.oag.go.ug/wp-content/uploads/2019/05/Identification-Registration-of-Persons-NIRA.pdf.*

22 Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness, Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons (Kampala: Unwanted Witness, 2021), 14, accessed 11 June 2021, *https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf.*

organisations. An extensive analysis of relevant pieces of Ugandan legislation was also conducted to explore the significance and provisions of the enabling statutes.

The analysis also relied heavily on the Centre for Internet and Society's *Framework for the Evaluation of Digital Identity*. The framework was used to guide the creation of sections, as well as terms useful for the evaluation of the ID framework in Uganda.

OVERVIEW OF THE IDENTITY LANDSCAPE

FOUNDATIONAL ID

In addition to NIRA, other ministries, departments or agencies that have oversight over ID systems in Uganda include:

- *the Office of the Prime Minister, Department of Refugees (OPM)*.[23] Uganda is the largest refugee-hosting country in Africa, with over a million refugees within its borders.[24] Under Section 8(1)(l) of the Refugees Act of Uganda,[25] the OPM is responsible for issuing "identity cards and recommendations for travel documents to refugees". The OPM is responsible for the Registration (refugee identity) number, a unique 12-digit number issued to all persons who have been registered in the Refugee Information Management System (RIMS), and for the refugee identity card;
- *the Ministry of Internal Affairs' Directorate of Citizenship and Immigration Control (DCIC)*.[26] The DCIC is responsible for the issuance of passports to citizens and visas, dependent passes, and work permits for foreigners, or an Alien Identification Card (AID) and
- *the Uganda Registration Services Bureau (URSB)*.[27] The URSB is responsible for marriage registration.

FUNCTIONAL ID

Functional IDs have been described as those "which evolve out of a single use case, such as voter ID, health records, or bank cards, and have potential for use across sectors".[28] Functional ID systems are different from foundational ID systems because they are developed for one specific purpose (or function) as opposed to foundational ID systems, which are designed for general purposes.

In Uganda, functional ID systems are useful for the authentication of service delivery, Know Your Customer (KYC) initiatives and other sectors requiring

23 The Office of the Prime Minister. *https://opm.go.ug/.*

24 Sulaiman Momodu, "Uganda stands out in refugees hospitality," United Nations Africa Renewal, *https://www.un.org/africarenewal/magazine/december-2018-march-2019/uganda-stands-out-refugees-hospitality.*

25 The Refugees Act, No 21 of 2006. *https://www.refworld.org/pdfid/4b7baba52.pdf*

26 "Directorate of Citizenship and Innovation," Ministry of Internal Affairs, accessed July 26, 2021, *https://www.immigration.go.ug/.*

27 URSB. *https://ursb.go.ug/*

28 World Bank Group, Digital Identity Toolkit: A Guide For Stakeholders In Africa, 4.

further identity authentication. Although Ugandan citizens previously had the use of a variety of functional IDs to access different services, these IDs have been replaced by the national digital identity project (NIRA/NSIS) and are no longer acceptable as proof of legal identity.[29]

The main stakeholders responsible for functional ID systems in Uganda include:

- the Electoral Commission of Uganda,[30] which is responsible for issuing the National Voters Card. Article 59(2) of the Ugandan Constitution[31] provides explicitly that it is the duty of every Ugandan over the age of 18 to register as a voter. However, the introduction of the foundational national digital ID program has seen the National Voters Card done away with. Also, because the Voters Register maintained by the Electoral Commission contains information available on the national ID card, it is impossible to vote without a national ID card;[32]
- other Ministries, Departments and Agencies (MDAs) that provide services, such as the Uganda Registration Services Bureau, the National Information Technology Authority Uganda, the Uganda Bureau of Statistics, and various security agencies. These MDAs are responsible for issuing driving permits, land registration records, medical health records, tax identification numbers (TINs), business registrations, and the like; as well as
- private sector actors such as telecommunication or mobile network operations, banks, insurance providers, among others, who are responsible for SIM card registration, and the issuance of insurance cards, credit or debit cards, etc.

PROCESS

The registration process for IDs is carried out by agents of NIRA. Enrolment and issuance of identity cards for first-time applicants are decentralised at the NIRA offices across the 117 districts of Uganda and the five divisions of Kampala. Applications for change of particulars and replacements were handled at the NIRA head office at Kololo for review, and were said to take one month if all

29 Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done?, 5.

30 Electoral Commission. *https://www.ec.or.ug/*

31 The Constitution of the Republic of Uganda, 1995. *https://www.parliament.go.ug/cmis/views/e138fbaf-95f5-4cbc-ac33-b4678be3577a%253B1.0*

32 Kikonyogo Douglas Albert, "How to know if your National ID Number is on the voters' register," *Tech Jaja*, 14 August 14 2019, *https://techjaja.com/know-if-national-id-number-on-voters-register/.*

information is in order.[33] Replacements have since been decentralised to the NIRA district offices since October 2018.[34]

Since only persons who are citizens, or can prove their citizenship through such preliminary documents as birth certificates, can apply for a national ID, the ID has become the most popular way of proving citizenship. To procure a national ID, applicants, who are citizens of Uganda, resident in or outside of the country, must fill out a NIRA form, and must prove citizenship through four main ways:

- Citizens by birth must show a copy of the national ID of both or either parent (if parents are alive) and a certified copy of a birth certificate. If these documents are missing, they must go through a lengthy, cumbersome procedure[35] to obtain a recommendation letter from the Local Council 1 (LC1 - the elected local government in districts) Chairperson stating that the applicant is a resident. The Chairperson also has to confirm the applicant's name, citizenship, tribe, clan, parental details, and the length of time the applicant has lived in the locality. Such recommendation letters must be signed with an official stamp of the LC1 Chairperson and the Gombolola (the Ugandan term for a sub-county) Internal Security Officer (GISO) or District Internal Security Officer (DISO).[36]
- In the case of people who hold dual citizenship[, applicants must produce a certified copy of their Certificate of Dual Citizenship and the passport issued by their current country of residence. (The certificate is issued once the application for dual citizenship has been granted.)
- Citizens by Registration must produce a certified copy of the Certificate of Citizenship by registration issued by the National Citizenship and Immigration Control Board (NCIB).
- Naturalised citizens must show a certified copy of the Certificate of Naturalisation as Ugandan issued by the NCIB.

The NIRA registration form, along with the supporting documents proving

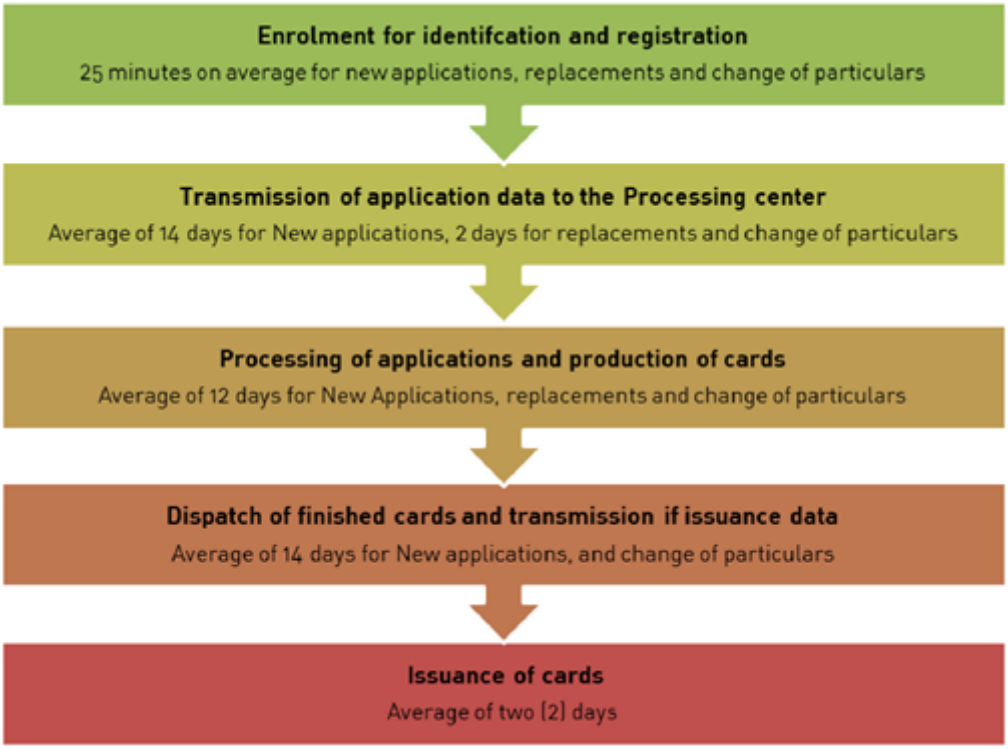
33 "Uganda - Correction of Information on an ID Card," Uganda, Wiki Procedure, accessed 20 August 2021, *https://www.wikiprocedure.com/index.php/Uganda_-_Correction_of_Information_on_an_ID_Card#Processing_Time.*

34 Office of the Auditor-General, A Value For Money Audit Report on the identification and registration of persons by the National Identification and Registration Authority (NIRA), 3.

35 Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness, Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 33-34.

36 Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done?, 7.

citizenship, are submitted to a NIRA registration official, who will verify and collect them for record purposes. After this is done, applicants are directed to the next station, where biometric information (fingerprints and high-resolution facial capturing) is gathered.



ID registration process in Uganda. Source: OAG Report 2018[37]

The ID registration process has been criticised for attempting to force an uneasy marriage between paper documentation processes, which would ordinarily require plastic cards inscribed with the information of the holder, and a digital biometrics system, which requires the digital scanning of fingerprints and facial features. This process, which excludes many, particularly senior citizens and manual labourers, as well as victims of disfiguring accidents, has been described as combining the worst of both worlds. It maintains, rather than eradicates, the onerous manual registration procedures used in paper documentation. This, coupled with the inability of digital biometrics systems to identify the relevant biometrics data in the cases mentioned above, results in a situation that has all the negatives and none of the positives.[38]

37 Office of the Auditor-General, A Value For Money Audit Report on the identification and registration of persons by the National Identification and Registration Authority (NIRA), 11.

38 Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 14.

Information required by NIRA for registration of the ID includes the applicant's name, date of birth, gender, information on citizenship, place of birth, details of parents, clan, tribe, ethnicity, spouse, education, tax information, personal biometrics information (including fingerprint or any other biometric information prescribed by the Minister), as well as any other information as may be required by the Authority from time to time. As this report discusses later, such extensive data collection is arguably contrary to the principles of data minimisation.

RULE OF LAW TESTS

3.1 LEGISLATIVE MANDATE

Registration of Persons Act

The primary law empowering and governing digital ID in Uganda is the Registration of Person's Act (ROPA), which was passed by the Parliament of Uganda in 2015. The ROPA mandates the compulsory registration of all persons living in Uganda, including aliens, in the National Identification Register.[39]

However, exceptions are granted to non-residents or Ugandan nationals visiting Uganda for up to 90 days, and persons who are recognised by the government and the United Nations High Commissioner for Refugees (UNHCR) to be refugees.[40]

The Act also establishes the government agency known as the National Identification and Registration Authority (NIRA) and outlines its functions, which are restricted to the creation, running and management of the national ID registration project.[41]

The Act also mandates other forms of registration, which provides for the compulsory registration of births,[42] and the compulsory registration of deaths.[43]

Section 66 of the ROPA provides that citizens who fail to register with NIRA are prevented from accessing services such as financial services, purchase of land and employment, among others. This is a clear violation of the individual's rights to dignity and privacy provided under Articles 24 and 27 of the Constitution of the Republic of Uganda. Non-registration is also criminalised under the Act as an offence liable on conviction to a fine not exceeding 120 currency points[44] or imprisonment not exceeding five years or both.[45]

By preventing Ugandan citizens from being able to make significant purchases such as land or obtain gainful employment, without a national ID, the Ugandan government is denying the right of its people to privacy from private persons, as

39 Section 54(a) and (b).

40 Section 1(2) (a) and (b).

41 Sections 4 and 5.

42 Section 28.

43 Section 41.

44 A "currency point" under Ugandan law is equivalent to UGX 20 000. In this example, a convicted person will be fined UGX 2 400 000 (120 times UGX 20 000) for not registering. That equates to roughly USD 680 at the 9 September 2021 exchange rate.

45 Section 76(a).

well as government officials and institutions.

It is also notable that although the Act was validly passed by the Ugandan Parliament, it grants vast, undefined powers to the Minister of the Interior, who is a member of the Executive, to make policy decisions including amendments and appointments under the Act.[46]

Data protection law

The Data Protection and Privacy Act (DPPA)[47] came into operation on 1 March 2019. The Act protects the privacy of individuals by regulating the collection and processing of personal information inside and outside Uganda, if the information relates to Ugandan citizens.[48] The DPPA also distinguishes between "special personal data" and "personal data".

Section 9 of the DPPA defines "special personal data" as data relating to the religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records of an individual. However, it does not impose additional obligations for protecting it.

As the statutory body established to coordinate and regulate Information Technology services in Uganda by the NITA-U Act 2009,[49] the National Information Technology Authority - Uganda (NITA-U)[50] is the regulator in charge of national data protection. The NITA-U is also mandated to maintain the Data Protection Register that lists every institution, person or public body that collects or processes the personal data of citizens and residents in the country. This includes the NIRA.

The DPPA defines "personal data" as any information about a person from which the person can be identified (such as identification number, occupation, nationality, age etc) that is recorded in any form. The rights of data subjects are set out through Sections 24 to 28 of the Act and include the right to access personal information; the right to know the purpose for which the information is being collected; and the right to prevent the processing of personal data, among others.

46 Sections 8, 65(1)(l), 66(2)(m), 84(1) and 85.

47 Data Protection and Privacy Act, No. 9 of 2019. *https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf.*

48 (Section 1 of Act No. 9 of 2019)

49 The National Information Technology Authority, Uganda Act, No 4 of 2009. *https://www.nita.go.ug/sites/default/files/publications/NITA-U%20Act%20%28Act%20No.%204%20of%202009%29.pdf.*

50 *http://www.nita.go.ug/*

Furthermore, Section 23 of the Act makes it mandatory for data collectors, data processors and data controllers to notify NITA-U of any unauthorised access or processing of data, as well as any remedial actions taken regarding such unauthorised access or use. However, NITA-U has the final say in determining whether data subjects may be notified of any such breaches.[51] Mandatory consent is required before collecting or processing personal data except where the collection is mandated by law, required for national security, service delivery by a public body, medical purposes or for compliance with a legal obligation to which the data controller is subject.[52]

3.2 LEGITIMATE AIM

Section 2 of ROPA itself defines its purpose as follows:

- removing duplication from the processes and laws relating to registration of persons;
- harmonising and consolidating the law on the registration of persons;
- establishing a central registration body (i.e. NIRA), for the registration of all persons in Uganda;
- establishing, a national identification register of all persons in Uganda; and
- providing for access and use of the information contained in the national identification register.

The World Bank's ID4D analysis[53] of the digital national ID project in Uganda describes the roles that robust, inclusive and responsible civil registration and identification systems play in providing citizens with a legal identity and generating vital and demographic statistics in today's digital world as an important justification for the project. Its report argues that the universal coverage of these systems can improve the accessibility, integrity, effectiveness and efficiency of public and private services.

As mentioned earlier, the national digital ID project sought to create a unified registry to merge various concurrent efforts by different arms of the government in preparation for the 2016 elections. It is also very likely, going by the original

51 Section 23(2), DPPA, 2019

52 Section 2, DPPA, 2019

53 World Bank, ID4D Country Diagnostic: Uganda (Washington DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 2018), 1, accessed 19 May 2021, *http://documents1.worldbank.org/curated/en/921761542144309171/pdf/132011-REVISED-PUBLIC-ID4D-Uganda-Diagnostic-12282018.pdf.*

name of the ID project, NSIS, that an underlying goal of the project was to create a comprehensive security database of all Ugandan citizens, ostensibly to improve national security and fight crime.[54]

In this regard, in 2021, the Ugandan government signed a 10-year contract with a Russian company, Joint Stock Global Security, to install mandatory global positioning system (GPS) trackers in all public and private vehicles, motorcycles and water vessels in the country. The Security Minister, Gen Jim Muhwezi, was quoted as saying, "The purpose of this Intelligent Transport Monitoring System (ITMS) is only one; it is security ...With this system, once there is a security situation, we will be able to tell which vehicles were in that place; there should not be any worry that there is going to be intrusion in the privacy of the motor vehicle users".[55] While this is still a developing story, it will be interesting to watch how the ID system will relate to the ITMS.

3.3 DEFINING ACTORS AND PURPOSE

Actors

In protecting citizens' privacy rights, it is important to properly define actors with access to the national digital ID system in the form of private or government officials or organisations.

One such actor, whose name is explicitly set out under the ROPA, is the Electoral Commission.[56] The Act authorises the Electoral Commission to use the information contained in the National Identification Register (NIR) to compile, maintain, revise, and update the voters register. Section 65(3) also provides that any ministry, department, or agency of government may also access and use the information contained in the NIR.[57] The decision of the NIRA to facilitate the sharing of personal data among government agencies has been criticised.[58]

The ROPA allows[59] private persons and organisations to access the information

54 Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 8.

55 Car trackers: Govt assures on privacy. Daily Monitor. Retrieved from *https://www.monitor.co.ug/uganda/news/national/car-trackers-govt-assures-on-privacy--3487014*

56 Section 65(2) of the ROPA.

57 See also Section 67(1) and (2).

58 NTVUganda, "ACCESS TO PERSONAL DATA: Government agencies gain access to NIRA database," May 5, 2018, video, *https://www.youtube.com/watch?v=EUmArhW-4e8.*

59 Section 67(3)

in the Register under Regulations[60] issued by the Board after consultation with the Minister. In 2017, in a move that was criticised,[61] the Ugandan government shared the biodata of registered persons with telecoms companies to ensure compliance with its compulsory SIM card registration efforts. Telecom providers were to verify the identities of subscribers against the NINs issued by NIRA. Following this, an incident involving the use of the NIN for financial fraud was reportedly traced back to the decision of the government.[62] However, this report was denied by the government.

Due to the centralised nature of the national digital ID project in Uganda, the access granted to private institutions and persons to the NIRA central database raises several concerns about the (mis)use of the information and access for commercially exploitative purposes. In a survey, 9.5% of respondents were found to have fears that their private information may be misused.[63]

The absence of the regulations meant to guide access to this information also gives some cause for alarm. Moreover, the existence of legislation such as the Anti-Terrorism Act[64] and the Regulation of Interception of Communications Act,[65] which empower secret services and the government to arbitrarily intercept data concerning or surveil persons in the country, also raises concerns.

Purposes

As the major purpose of the ROPA is the registration of persons in Uganda, there are no limitations to the uses for which the ID may be required. The Act aims to ensure that all citizens are registered and accounted for. Also, the data collection

60 Registration of Persons Regulations, No 67 of 2015. *http://ugandanlawyer.com/wp-content/uploads/2019/03/Registration-of-persons-regulations-2015.pdf*

61 "Sharing of the national identity card database with private telecoms is prone to abuse/misuse," Unwanted Witness, April 4, 2017, *https://www.unwantedwitness.org/sharing-of-the-national-identity-card-database-with-private-telecoms-is-prone-to-abusemisuse/.*

62 "Unwanted Witness Condemns the criminal use of citizens' bio data & calls on gov't to formulate safeguards to protect lives and property," *Unwanted Witness*, 26 June 2017, *https://www.unwantedwitness.org/unwanted-witness-condemns-the-criminal-use-of-citizens-bio-data-calls-on-govt-to-formulate-safeguards-to-protect-lives-and-property/.*

63 Resilient Africa Network, Understanding the Benefits, Costs, and Challenges of the National Identification System in Uganda: Findings from a Household Survey and a Costing Study (Kampala: USAID, 2019), 35, accessed July 28, 2021, *https://www.ranlab.org/wp-content/uploads/2020/10/Understanding-the-Benefits-Costs-and-Challenges-of-the-National-Identification-System-in-Uganda-1.pdf.*

64 The Anti-Terrorism Act, 2002. *http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf*

65 Regulation of Interception of Communication Act, No 18 of 2010. *https://chapterfouruganda.org/sites/default/files/downloads/Regulation-of-Interception-of-Communication-Act-2010.pdf*

and registration processes and requirements make no distinctions between what type of data is strictly necessary for beneficial purposes, nor does it make allowances for requesting the submission of data in order to access various services. For instance, it is difficult to understand the relevance of information about a person's clan, ethnicity and descendants when they want to open a bank account. Essentially, there is no opportunity for individuals to determine what information is strictly necessary while attempting to access certain services.

Schedule 3 of the Act provides for the type of information required at registration as follows:

- name and date of birth;

- information relating to citizenship and details of such citizenship;

- information relating to—

- place of birth;
- details of parents;
- clan;
- descendants;
- tribe;
- ethnicity;
- sex;
- marital status;
- details of spouse where applicable;
- education and profession;
- occupation;
- address;
- tax identification numbers;

- passport number, where applicable;

- personal biometric information, including fingerprint or any other biometric information prescribed by the Minister; and

- any other information as may be required by the Authority from time to time.

The extensive amount of information required for registration purposes is arguably directly at odds with the principle of data minimisation, which is "the practice of limiting the collection and processing of personal information to what is directly relevant and necessary to accomplish a specified purpose".[66] It is questionable if information about an individual's clan and ethnicity, for instance, should be relevant to them acquiring a legal identity.

Data minimisation is also supported by the Data Protection and Privacy Act 2019,[67] which provides that data collectors, data processors, data controllers or any person who collects, processes, holds or uses personal data shall only do so to gather adequate, relevant data and not excessive, unnecessary personal data. Section 12 of the DPPA goes on to provide that any person who collects personal data shall do so for a lawful purpose, which is specific and explicitly defined.

Considering that the DPPA came into force after the Registration of Persons Act, its provisions ought to supersede those of the latter. However, the provisions of the DPPA have yet to be complied with, due to a lack of political will as evidenced by the government's failure to amend the provisions of the ROPA.[68]

3.4 REDRESS MECHANISM

User notification

While user notification is a valuable tool for potentially improving data accountability, the ROPA provides no provisions for the notification of data subjects when a data breach occurs or when their data is used or accessed by public or private agencies.

Section 23 of the DPPA does, however, stipulate that when a data breach occurs, the data collector, processor or controller should immediately notify the Authority, who will then determine if the data subject is to be notified of the breach. If the Authority determines that the data subject is to be notified, they shall be contacted via post, email, website notification or publication in mass media with sufficient information to allow them to take protective measures against the breach.

In addition to this, Regulation 33(1) of the Data Protection and Privacy

66 "Data minimisation," Glossary, Thomson Reuters - Practical Law, accessed 27 July 2021, *https://uk.practicallaw.thomsonreuters.com/w-014-9030?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true*

67 Section 3(1)(c)

68 "One Year On, what has Uganda's Data Protection Law Changed?," Privacy International, last modified 3 March 2020, *https://privacyinternational.org/news-analysis/3385/one-year-what-has-ugandas-data-protection-law-changed*

Regulations 2021[69] provides that the notification be made immediately after the occurrence of the data breach.

Under Section 56, the ROPA provides that the Minister may give notice by publishing, in the Gazette or mass media, the deadlines for registration under the Act. Regulation 16 of the Registration of Persons Regulations of 2015 also provides that whenever the NIRA refuses to register a person, it must inform the person about its decision and reasoning within 30 days. A person who is dissatisfied with the NIRA's decision may appeal to the registration and identification committee, and further appeal the Committee's decision, within 30 days to the High Court.[70]

In addition to this, if there is any cause to cancel the registration of a person under Section 57, the NIRA has to notify the person of its intention to cancel their registration and provide them with reasonable opportunity and forum to show cause why the registration should not be cancelled. However, in these two scenarios neither the Act nor the Regulation specifies how a person will be notified.

While the Act and Regulation are both silent on grounds that may lead NIRA to refuse a person, it may be inferred that non-compliance with registration requirements would be grounds for refusal. The Act stipulates[71] that the registration of a person may be cancelled where:

- a person has, under the law, ceased to be a citizen of Uganda;
- the registration is based on inaccurate or incomplete information;
- the registration was obtained by fraud, false representation, bribery or deceit;
- the card needs to be re-issued due to a defect;
- double or multiple registrations have taken place; or
- there is a court order for cancellation of registration

In practise, though, applicants are only informed of any issues when they return to pick up their cards.[72] This implies that there is either no way to contact data subjects (due to a lack of technical or financial resources) or there is an unwillingness to do so despite the relevant novel provisions in the DPPA and ROPA stipulating it.

69 The Data Protection and Privacy Regulations, 2021. Statutory Instrument 21 of 2021. *https://www.dataguidance.com/sites/default/files/uganda_data_protection_regulations_small.pdf*

70 Regulation 16(2) and (3), Registration of Persons Regulations, No 67 of 2015

71 Section 57 of the Registration of Persons Act.

72 Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done?, 7.

Access and correction

The ROPA makes no provision for registered persons to access or request whatever information has been processed about them. However, some provisions regarding the procedure to correct the information exist.

For instance, Section 51 of the Act provides that the Executive Director may authorise the staff of the NIRA in writing to correct any error in the register, return, index or certificate. This is particularly useful in situations where the errors on the national ID card are obvious, as in the case of sex or age. Section 64(3) furthermore provides that people notify the Authority of any change or error in the information recorded about them. However, this provision is not couched as a right but rather as a duty or responsibility on the individual. Failing to notify the NIRA of changes could lead to a fine, imprisonment or both upon conviction.

The DPPA does provide for the rights of data subjects to correct or delete and access their personal data upon verification of their identity.[73] While the provisions of the DPPA ordinarily ought to supersede the provisions of the ROPA, in practice, neither the Data Protection Office created under the DPPA nor the NITA-U are independent bodies. Both fall under the general supervision of the Minister of Information and Communication Technology.[74] This severely limits the power of the DPPA and constrains its implementation.

Due process

Generally, the ROPA makes provision for redress at the High Court[75] whenever a person is dissatisfied with a decision of the Identification and Registration Committee. The Committee, which is established by the Board of NIRA, presides over matters arising and/or related to registration under the Act, such as complaints.[76] This is in conjunction with Section 15(1) which provides that the

73 Sections 16 and 24 of the DPPA

74 Unwanted Witness, Data Protection and Privacy Law Analysis (Kampala: Unwanted Witness, 2019), 3-4 accessed 27 July 2021, *https://www.unwantedwitness.org/download/uploads/Data-Protection-and-Privacy-Law-Analysis.pdf*

75 The High Court of Uganda is the third court of record in order of hierarchy after the Court of Appeal and the Supreme Court. It has unlimited original jurisdiction, which means that it can try any case of any value or crime of any magnitude. Appeals from all Magistrates Courts go to the High Court.

76 Section 83 of the ROPA.

Board may appoint committees as follows:

> (a) to inquire into and advise the Board on any matter concerning the functions of the Authority as the Board may refer to the committee;
>
> (b) to exercise such powers or perform such functions of the Authority as the Board may delegate or refer to the committee.

Section 83(3) also provides that offences under the Act, such as failing to register or providing false information when registering,[77] shall be tried by the High Court.

3.5 ACCOUNTABILITY

The closest thing to systems for accountability provided under the Act are the provisions of Section 5(2) which provide that the NIRA shall observe generally accepted information security practices and procedures, and specific industry or professional rules and regulations. Notably, however, it does not specify what these practices and procedures are nor does it specify the consequences of non-compliance.

Section 61 also provides for the non-disclosure of information by registration officers. It provides that a registration officer or a person, who processes personal data on behalf of the Authority, shall treat the information which comes to the knowledge of the person as confidential and shall not disclose the information unless required by law.

The Registration of Persons Act 2015 grants immunity to staff under Section 82. This undermines efficiency and accountability among agents of the Authority, leaving no room for administrative or legal procedures to seek redress against staff for registration errors. Replacement or correction of errors also comes with a cost to citizens of UGX 50 000 (around USD 14).

However, when a direct comparison is made between Section 61 and Section 82, which grants immunity to employees of the Authority, the provisions contained in the former appear to be merely normative and ineffectual and not sufficiently compelling. The latter, in particular, could impede accountability, especially as it does not explicitly criminalise the disclosure of such information or set out how the law may require the information to be disclosed.

Although the ROPA does not contain many provisions regarding accountability, there are certain provisions in the DPPA to similar effect. For instance, Section 21 of the DPPA provides that where a data controller, in this case NIRA, engages third party data processors, NIRA as the data controller is required by the DPPA

77 Section 76(a) and (b) of the ROPA.

to draw a contract with the data processor requiring it to establish and maintain confidentiality and security measures necessary to protect personal data. Regulation 32 of the Data Protection and Privacy Regulation also provides that data controllers must ensure that data processors develop and implement the appropriate security measures to protect personal data.

Furthermore, according to Section 22 of the DPPA, when a third party processes personal data on behalf of a data controller, in this case NIRA, it must do so only with prior knowledge and authorisation.

Other sections providing for accountability include:

- Section 3(1) of the DPPA, which says that data controllers, data processors, data collectors or any other persons who collect, process, hold or use personal data are accountable for data collected and processed;
- Section 10 of the DPPA, which provides that processing of personal data must be done in a way that ensures that the right to privacy is not infringed;
- Section 20(3) of the DPPA, which provides that data controllers shall observe specific professional rules and regulations and security practices and procedures;
- Section 31 of the DPPA, which provides that a data subject may make a complaint in the case of a breach or non-compliance with the Act; and
- Section 23 of the DPPA, which provides that a data subject is entitled to apply to a court of competent jurisdiction to seek compensation for distress or damage caused by data controllers, data processors and data collectors.

3.6 MISSION CREEP

Mission creep has been defined[78] as the gradual broadening of the original objectives of a mission or organisation.

The digital ID project in Uganda, being a foundational ID system, is designed to govern and encompass all aspects of an individual's identity. It is therefore unsurprising that the Act does not specifically criminalise or make provisions to prevent mission creep.

In fact, the Act provides that other agencies of the government may use the collected data for "related purposes". Section 65(1)(l) of the ROPA provides that the information collected in the register may be used for any other purpose as may be determined by the Minister responsible for Internal Affairs. Section 65(3)

78 "Mission Creep," Merriam-Webster, accessed 20 August 2021, *https://www.merriam-webster.com/dictionary/mission%20creep.*

then goes on to provide that a ministry, department or agency of the government may access and use the information contained in the register for the purposes contained in Section 65(1). This particular Section appears to be the justification behind the decision of the police force to make use of the data collected by NIRA to fight crime and improve surveillance. In the words of an ICT police officer, "We're not setting up the system for only NIRA and police, but also the DPP [Director of Public Prosecutions] office and court will be able to get details of suspects or convicts at any time by just typing in the person's name... This is why we (are) also profiling every person involved in capital offences."[79]

Although Section 67(1) of the Act limits access to the information in the register to information required by a ministry, department or agency of the government, this provision is countered by Section 67(3), which provides that a person other than a ministry, department or agency of Government may access the information in the Register under discretionary regulations issued by the Board. While the Registration of Persons Regulations have since been passed, they contain no guidelines on how MDAs may access information in the Register.

Example of mission creep

In March 2021, prior to the rollout of the vaccination campaign against Covid-19, the Permanent Secretary of the Ministry of Health tweeted that only those with national identification cards or NINs will have access to the vaccine offered by the Ministry of Health in Uganda. Several prominent civil society organisations protested that this would undermine the fundamental right to health and is in contravention to several international instruments that Uganda is a party to. Following the outcry, the requirement for identification was withdrawn by the Ministry of Health.[80]

79 "Police building technology interface with NIRA to access data," The Independent, 16 March 2021, *https://www.independent.co.ug/police-building-technology-interface-with-nira-to-access-data/.*

80 Initiative for Social and Economic Rights, ISER Welcomes The Ministry Of Health Decision To Withdraw The National ID Requirement for Covid 19 Vaccination (Kampala: Initiative for Social and Economic Rights, 2021), accessed August 20, 2021, *https://www.iser-uganda.org/images/downloads/ISER_welcomes_MoH_withdrawal_of_National_ID_requirement_for_Covid_19_Vaccination.pdf*; Ministry of Health, PRE-COVID-19 VACCINATION PRESS BRIEFING (Kampala: Ministry of Health, 2021), 4, accessed August 20, 2021, *https://www.health.go.ug/download-attachment/d2Upa2r7q1f_3IlhGKtXcbLfBFgGNSxumvv-6DWdH-Y.*

RIGHTS-BASED TESTS

4.1 NECESSITY AND PROPORTIONALITY

While Article 27 of the Constitution of Uganda provides for the right to privacy of persons, homes and other property, several provisions of the Registration of Persons Act contain stark infringements of this right.

The most significant challenge to privacy and autonomy is that the registration of persons is not voluntary, but compulsory. Section 54 of the ROPA provides that all citizens of Uganda, whether resident inside or outside Uganda as well as alien residents issued with a permit, certificate or pass under the Uganda Citizenship and Immigration Control Act must be registered. The penalty for failure to register is a fine of up to 120 currency points[81] or imprisonment up to five years or both.[82] Although no one has yet been arrested for failure to register under the ROPA, the inability to access important services such as healthcare[83] is enough to compel many to register.

The risk of privacy breaches is also compounded by the means through which information is stored. Under the registration scheme, information storage is centralised under the National Security Information System (NSIS) Project designed and intended to be the sole means of deploying legal identity for citizens. This could create vulnerabilities for data protection and misuse by third parties.

Justification for the ID project comes in form of the results and benefits accruable to citizens who have legal identity. However, the benefits of the ID system are outweighed by the existence of Section 66 of the Act preventing anyone without a national ID card or number from accessing basic services. There is clearly an imbalance in the benefits accruable to citizens under the scheme because the ID card strips away several of the fundamental rights already afforded to Ugandan citizens under the Constitution, while demanding an extreme amount of information, to grant them - again - access to those very rights

81 A currency point is equivalent to 20000 Ugandan Shillings.

82 Section 76.

83 Samuel Okiror, "Uganda's ID scheme excludes nearly a third from healthcare, says report," Guardian, June 9, 2021, *https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report.*

and risks fomenting exclusion against persons unwilling or unable to register. The provision for the mandatory use of the national identification cards only as the sole valid identification to access various services in the country, across both private and public sectors, ensures that it is easy to profile and surveil citizens since only one central form of identification is tied to them.

Mandatory use

The Act does not explain the justification for the mandatory acquisition of and registration for the digital ID (for which criminal and administrative sanctions exist) beyond the general aims and purposes stipulated at the beginning of the Act. For instance, Section 76 provides that anyone who fails to register commits an offence and is liable on conviction to a fine not exceeding 120 currency points or imprisonment not exceeding five years or both. Similarly, Section 66 of the Act means that anyone without a national ID is unable to access several services ranging from bank services to employment, insurance, pension transactions and any other type of service prescribed by the Minister. Recently, members of civil society instituted court action against the Government of Uganda over the requirement to have a national ID card before receiving the Covid-19 vaccine.[84]

The mandatory nature of the Ugandan ID system being a foundational identity system poses troubling questions for several rights, including but not limited to privacy, dignity, autonomy, and consent. In addition, there is a high risk of exclusion from accessing basic social services - such as accessing student loans, gaining employment, opening bank accounts or registering for a SIM - where the national ID is made mandatory.[85] There is a possibility that citizens may miss out on crucial services such as medical services as well. For example, in 2018 the health minister informed the public of the government's plan to "[set] up a digital system with in-built mechanisms to, among other things, enable pharmacies not to dispense drugs to patients without national IDs".[86] The absence of a valid

84 Initiative for Social and Economic Rights and Unwanted Witness, Civil Society Drags Government To Court Over Requirement To Have National ID Card Before Receiving Covid 19 Vaccine (Kampala: Initiative for Social and Economic Rights and Unwanted Witness, 2014), accessed 27 July 2021, *https://www.iser-uganda.org/images/downloads/COVID19_vaccine_and_IDs-ISER_Press_Briefing.pdf.*

85 Unwanted Witness, Uganda's Digital ID System: A cocktail of Discrimination (Kampala: Unwanted Witness, 2020), 6, 28, accessed 19 May 2021, *https://www.unwantedwitness.org/download/uploads/UgandaE28099s-Digital-ID-System.pdf.*

86 Privacy International, "How national ID systems make social protection inaccessible to vulnerable populations," IFEX, last modified 12 April 2021, *https://ifex.org/how-national-id-systems-make-social-protection-inaccessible-to-vulnerable-populations/*

reason for the invasive nature of the information required is bothersome as well, especially as there are no alternative forms of identification permitted to access various services as prescribed under the Act.

4.2 DATA MINIMISATION

The provisions of the DPPA[87] protect against the collection of data for extrinsic purposes as well as against the retention of data beyond the specified period.

Section 3(1)(c) and (d) of the DPPA provide that a data collector, data processor, data controller or any person who collects, processes, holds or uses personal data shall only process adequate, relevant data and not excessive or unnecessary personal ones. In addition, personal data shall only be retained for the period authorised by law or for which the data is required.

Section 12 provides that a person who collects personal data shall do so for a lawful purpose that is specific, explicitly defined and is related to the functions or activity of the data collector or data controller.

In a similar vein, Section 18(1) of the DPPA provides that a person who collects personal data shall not retain it for longer than necessary. However, further reading of the Act reveals that there are significant exceptions to this principle that are capable of curtailing its effectiveness. These exceptions are listed in Section 18(2)(a) to (f) and they include the prevention, detection, investigation, prosecution or punishment of an offence or breach of law[88] as well as national security purposes.[89]

The foregoing, when jointly read with the provisions of the ROPA[90] that compel the registration of all citizens, appears to merely pay lip service to the principle of data minimisation. It is difficult to understand the necessity of some of the required information, especially when the risks of data breaches, readily apparent in the centralised information storage system operated in the country, are weighed.

4.3 ACCESS CONTROL

Another troubling angle to the breach of privacy inherent in the ID system is poor access controls, due to minimal or no restrictions on collected data by state

87 Section 3(1)(c) and (d) and Section 12.

88 Section 18(2)(a)

89 Section 18(2)(b)

90 Schedule 3 of the Act.

or private agents. According to Section 65(3) of the Act, a ministry, department or agency of the government may access and use the information contained in the register for the purposes listed under Section 65(1), described above. The stated purposes are, however, open-ended and may include whatever purposes are designated by the Minister of Interior.[91] This provision, in particular, provides unfettered administrative powers to the Executive arm of the government via the Minister, and may itself be a breach of the principle of separation of powers among the three arms of government.

Unsurprisingly, Section 65 provides no rules or guidelines regarding the process by which access to the information may be procured by different state agencies nor how data subjects may be notified of it. It also provides no procedure (or procedural safeguards) for the exercise of the Minister's power to include novel purposes under it. It does however provide[92] that "a registration officer or any other officer of the Authority who without authority discloses, submits or transfers data from the register to any other person, commits an offence and is liable on conviction to a fine not exceeding [72] currency points or imprisonment not exceeding five years or both."

While Section 67(1) of the Act limits access to the information in the register to information required by a ministry, department or agency of the government, Section 67(3) provides that a person, such as members of the private sector, other than a ministry, department or agency of government may access the information in the register under regulations issued by the Board after consultation with the Minister. Notably, these regulations are not explicitly set out in the Act itself and could therefore be discretionary.

Section 31 of the DPPA, however, provides that complaints about data breaches and non-compliance should be made to the NITA. Section 33 goes on to provide that where a data subject suffers damage or distress, through the actions of a data processor, controller or collector, in contravention of the DPPA, the data subject is entitled to seek redress in a court of competent jurisdiction. Section 34 then provides that where a person is dissatisfied with the decision of the NITA, they may apply to the Minister. An action reflective of the lack of independence of the NITA itself.

Under the Registration of Persons Regulation, however, recourse to the High Court to challenge the Identification and Registration Committee's decisions is only explicitly provided for under three circumstances:

91 Section 65(1)(l)

92 Section 81

- where a person is dissatisfied with the decision of the Committee regarding the change of information in the register;[93]
- where a person is dissatisfied with the refusal of the Committee to register a person;[94] and
- where a person is dissatisfied with the decision of the Committee to cancel or revoke a person's registration or its refusal to register a person.[95]

It is not clear why the decision of the Committee may only be challenged under these three circumstances, even though they appear to cover the majority of reasons for which dissatisfaction might arise under the registration process. In addition, there is no evidence that this Committee has ever been set up or carried out the duties assigned to it under the Act, a likely explanation for the dearth of court cases challenging the provisions of the Act and the NIRA.

93 Regulation 4.

94 Regulation 16.

95 Regulation 17.

RISK-BASED TESTS

5.1 RISK ASSESSMENT

Privacy harms

Conducted in 2018, the World Bank's ID4D[96] assessment report on the Ugandan national digital ID project outlined a number of privacy and data protection concerns and recommendations regarding the project.

In particular, the report recommended the passing of a Data Protection and Privacy Act (which has since happened) as well as provisions for the safeguarding of data privacy, security and user rights through a comprehensive legal and regulatory framework. While the DPPA[97] does task data controllers, i.e. NIRA, with conducting regular audits and other safety measures to secure the integrity of personal data, the full implementation of its provisions remains a challenge.

However, data protection principles contained in the DPPA appear not to have been embedded in the ID system, in light of the data of citizens routinely being shared across platforms by NIRA subsequent to the passing of the Act.[98]

Exclusion harms

The World Bank's report also outlined[99] certain potential exclusionary risks resulting from the ID project such as:

- the exclusion of out of school children from the Registration of Learners[100] project. This initiative by the Ugandan government was created to promote the registration of children in schools under the national ID project;
- the impact of card replacement costs on indigent people who live far away from urban areas; and
- financial exclusion driven by KYC initiatives in financial institutions, as well as the use of manual verification procedures through documents such as utility bills, by banks, due to the inability to digitally verify the national

96 World Bank, ID4D Country Diagnostic: Uganda, 37-39.

97 Section 20.

98 Privacy International, "One Year On, what has Uganda's Data Protection Law Changed?".

99 World Bank, ID4D Country Diagnostic: Uganda, 20-21, 30.

100 *https://www.nira.go.ug/index.php/registration-of-pupils-and-students/*

ID as a result of a lack of access to the NIRA's database.

Recent reports[101] do not show a marked improvement in the delivery of services following the establishment of the national digital ID project, possibly due to the absence of stable internet connectivity and imperfect biometric authentication. These issues continue to pose difficulties for Ugandan citizens.

The following cases of exclusion at the registration process were identified as part of this report:

- *Persons with disabilities*: People who were unable to present their fingerprints due to disability, were turned away from the NIRA registration offices and were not able to receive their IDs. Provisions need to be made to cater to the needs of differently abled individuals, as many other countries do. For example, in Tanzania, there is a clear course of action in the Tanzania Registration and Identification of Persons Regulations 2014[102] which provides for the collection of alternative biometric information when disability renders it impractical to collect the prescribed information such as fingerprints. The Tanzanian law permits the use of a palm, toe prints or any other special identification mark instead of a fingerprint.
- *People in traditional marriages*: During registration for national ID, individuals are asked if they are married and, if so, they are required to produce a marriage certificate. This requirement can only be met by people married in a church or in a civil marriage at the Magistrate's Courts. Couples married (only) traditionally in most areas of Uganda (except Buganda) do not receive marriage certificates. Thus the requirement of a marriage certificate makes it difficult for a traditionally married couple to register for the national ID.
- *People living in remote areas*: Persons who live in remote areas are often unable to afford the costs involved in traveling to NIRA district offices, which may involve several trips to gather all the requisite information. Although there have been attempts to decentralise the registration process to ease transportation and other attendant costs on people living far from urban areas, these attempts have been plagued by underfunding and human resource gaps.[103] Moreover, although there are no costs attached

101 Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done?, 7.

102 Registration and Identification of Persons Act, Regulations, 2014. *http://citizenshiprightsafrica.org/wp-content/uploads/2020/01/Tanzania-Registration-and-identification-of-persons-regulations-2014.pdf*

103 Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done?, 7.

to the original registration procedure, a survey conducted by Unwanted Witness revealed that 25% of applicants paid a bribe to get registered for the national ID, in addition to costs paid acquiring supporting documents.[104] Analysis of the report also revealed that although persons were aware that technically, the registration process was free, they felt compelled to pay the bribe to hasten the processing of the ID card so that they could access loans or make travel plans.[105]

- *Aged people*: Many aged persons in Uganda, a majority of whom live in rural areas, are unable to travel to NIRA offices to register for their IDs. Additionally, older persons tend to provide incorrect information at registration, especially on their date of birth which they might not know. This later hinders their access to services and benefits to which they are entitled. Changing this information at a later time adds additional costs and emotional strain.
- *Women and girls*: The GSMA Digital Identity programme[106] identified unique barriers women face when accessing and utilising national IDs in 10 countries across the world. While there is currently insufficient data on this gender gap, the same issues that impact people in remote areas and the aged (such as distance, time and costs) are likely to affect women's and girls' attempts to register for an ID. The mandatory SIM registration in Uganda that requires a national ID has been a major driver in uptake of the ID. However there is also a digital gender gap, which is evident in mobile money uptake, a principle method of accessing financial services for the unbanked. Only 35% of women in the country over the age of 15 use mobile money services compared to around 49% of men.
- *Minority groups*: The Maragoli, an ethnic group living in the Kiryandongo district, have been claiming recognition as Ugandans but, in some counties, members of the group were denied national IDs by the NIRA.[107] Although the Maragoli were absent in the national schedule of the 1995 Constitution and the 2005 amendment, they had been granted the same rights as all Ugandan citizens until the Registration of Persons Act 2015

104 Unwanted Witness, Uganda's Digital ID System: A cocktail of Discrimination, 26.

105 *Ibid.*

106 Exploring the Gender Gap in Identification: Policy Insights from 10 Countries (2019) *https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/04/Exploring-the-Gender-Gap-in-Identification-Policy-Insights-from-10-Countries-Web.pdf*

107 Bamuturaki Musinguzi, "Maragoli Minority Group to be Recognised Soon," Daily Monitor, 11 April 2021, *https://www.monitor.co.ug/uganda/news/national/maragoli-minority-group-to-be-recognised-soon-3358160.*

was passed. They are now denied their IDs if they refuse to register under a listed tribe, such as the Banyaro or Alur.

- *Out-of-school children from the Registration of Learners project*: A recent World Bank report[108] indicated that children who were out of school during the national ID period risked being excluded from the project due to its focus on schools and school children. Subsequently, the government announced that there would be no special intervention programmes to register out-of-school children as they would, instead, be registered during the general continuous registration exercise at public centres. This may further lower their chances of acquiring a legal identity and limit their access to public services.[109]

Unsurprisingly, access to financial services is severely limited without the national ID card which has affected the KYC originally required by banks. Banks, in particular, most frequently require the national ID to provide requested services.[110] Elderly people also face financial exclusion when they are prevented from receiving their pensions or aid under schemes such as the Senior Citizens Grant (SCG) and Social Assistance Grants for Empowerment (SAGE) for lack of a national ID.[111]

Reports[112] show that groups such as the elderly or manual workers who have had their fingerprints eroded are often turned away with no alternative means of gaining a legal ID . This is due to NIRA's inability to offer biographic verification services[113] for access to and delivery of services. The same situation occurs with people who, due to facial disfigurement, are unable to undertake facial capturing. Language barriers also exist and prevent staff from registering many people who do not understand English, as all forms are available in English only.[114]

These realities are worsened by Section 66 of the Act which provides that ministries, departments or agencies of the government or any other institution

108 World Bank, ID4D Country Diagnostic: Uganda (Washington DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 2018), 1, accessed 19 May 2021

109 https://www.nira.go.ug/index.php/contact-us/faqs/

110 *Ibid*, 28.

111 Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 30.

112 *Ibid*., 7.

113 World Bank Group, The State of Identification Systems In Africa: Country Briefs (Washington DC: International Bank for Reconstruction and Development / The World Bank, 2017), 57, accessed 7 October 2017, *https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y.*

114 English is the official language of Uganda

providing a public service shall require a person accessing the service to produce a national identification number or national identification card or alien's identification number or alien's identification card. This leads to exclusion due to the difficulty involved in the registration process.

Section 66(2) of the Act also sets out a list of services which require ownership of the digital ID as a prerequisite for service provision and access. These services include employment, the opening of bank accounts and pension transactions. The impact of these regulations on the inclusion and exclusion of the disabled, on senior citizens as well as on women seeking sexual and reproductive healthcare is immense and is worsened by the surrounding failure and refusal to offer alternatives ways to access these services.

Discriminatory harms

Discrimination against refugees was outlined as an exclusionary risk by the World Bank's report, especially since refugees are not permitted to register under the ROPA.[115]

Discrimination against female Ugandans who are unable to access sexual and reproductive healthcare without a national ID card is particularly rampant and harmful.[116] Ugandan women who sell charcoal or pick aloe plants have been unable to register due to the erosion of their fingerprints. Senior citizens are subjected to degrading remarks as a result of cultural stereotypes. In a Parliamentary hearing, it was remarked as follows, "We have people who do not have the print. In Luganda, we can call it "Njola". Someone goes there with a thumb, most especially old people, they try to capture it and it cannot be captured. I have seen them being chased. One time, I witnessed an old man being told to go and look for spirit [surgical alcohol], clean the place and come back. It was not even provided there but they told the old man to go away".[117]

Persons who are not in possession of the ID are also considered suspicious and possessing criminal intent.[118]

115 Section 1(2)(b).

116 Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 54.

117 Hansard Parliamentary Debates (Uganda), 11 March 2020, 22. *https://www.parliament.go.ug/cmis/views/e0bf0740-8668-47dd-b962-9704fea9a47f%253B1.0*

118 Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, 9.

5.2 DIFFERENTIATED APPROACHES TO RISK

Per se harmful and not harmful

While the ROPA does not define factors or incidents which are especially harmful or harmless nor distinguish between them, Section 20 of the DPPA provides that data controllers, collectors and processors must secure the integrity of personal data in their control or possession by adopting appropriate measures to prevent loss and unauthorised destruction, processing or access to personal data.

Regulation 12(1) of the Data Protection and Privacy Regulations provides that:

> *"where the collection or processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the data collector, data processor or data controller shall, prior to the collection or processing, carry out an assessment of the impact of the envisaged collection or processing operations on the protection of personal data."*

Regulation 12(3) goes further to provide that the Personal Data Protection Office "shall establish and make public a list of the processing operations which are subject to the requirement for a data protection impact assessment under sub-regulation (1)." However, the Data Protection Office is yet to do so.

Sensitive uses

While the DPPA[119] sets out a list of what is to be considered "special personal data" (namely data relating to: religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records of an individual), under the ROPA, there are no provisions to operationalise or give effect to this distinction by providing higher protection to special personal data.

The relevant sections of the ROPA mandate the comprehensive collection of data about citizens and residents in return for the ID.[120] This is especially apparent in the mandatory nature of the national ID project, which is devoid of alternative methods that are needed to overcome existing physical and infrastructural challenges.

119 Section 9.

120 Section 57.

5.3 PROPORTIONALITY

Inaccurate data collection

As Sections 32, 34 and 51, 53 of the ROPA clearly reveal, some consideration of the risk posed by inaccurate data collection has been taken into account by the regulatory authority, especially as the risk of inaccurate data collection is high.[121]

For instance, Sections 32 and 34 place a burden on registering officers to verify and indicate the correctness of information in the birth certificate, while Sections 44 and 45 reflect the same burden in the registration and validation of the death certificate.

In the same vein, Section 53 punishes the entering of false information in the register by a fine not exceeding currency points or to a term of imprisonment not exceeding six months.

The Act also makes provision for the correction process under Section 51 of the Act. The Section allows the Executive Director of NIRA to authorise NIRA staff in writing to correct any error in the register, return, index or certificate. However, Sections 4 and 5 of the Registration of Persons Regulations, 2015, provide alternative procedures for correction. The Sections make provisions for procedures through which the NIRA may be notified in the event of any changes or errors in the information in the register.

The incongruity in the provisions of the Act and the Regulations could be pointing to an administrative procedure in the case of the former and an individual one in the case of the latter. Hence the Act may refer to departmental or organisational errors and the latter to personal, unauthorised errors. It is, however, unclear if they are two stages in the correction process, or wholly unrelated methods distinct in their uses. This uncertainty poses a financial stumbling block to individuals who might be interested in correcting the information recorded about them but reside in remote areas and present them with challenges to choose the better approach to take.

Authentication errors

To mitigate the risk of authentication errors under the ID project, the ROPA provides for the issuing of NINs[122] to all persons registered in the registry, and for

121 "National ID errors make elderly miss SAGE cash," Daily Monitor, July 11, 2020 *https://www.monitor.co.ug/uganda/special-reports/national-id-errors-make-elderly-miss-sage-cash-1899228*

122 Sections 5(e) and 68.

the issuing of an Alien Identification Number[123] to a child identified as an alien.

The NIN serves as an alternative to biometric identifiers when applying or registering for certain services requiring ID registration. The allocation of the NIN in place of biometric identification would, in addition to minimising data collection, remove authentication errors frequently encountered with facial or fingerprint capturing. However, it is impossible to register for the national digital ID - and by extension for the NIN - without the collection of biometric identification in the form of fingerprints because the collection of biometric identification is part of the registration process.

Relatedly, under Section 68(2) of the Act, production of the NIN is *prima facie* evidence of citizenship.

Mission creep

As mentioned above, Sections 65 and 67 of the ROPA show worrying tendencies for mission creep in the functions of the Authority.

The provisions of the Act do not contain any apparent considerations for the severity or risk of mission creep. On the contrary, it appears that interoperability and mission creep are welcomed and anticipated in its provisions.

Regarding the legal redress of grievances, as a general rule, Section 82 of the Act provides immunity to members of the Board, staff of the Authority or persons acting under the authority of the Board or of the Authority itself. However, in specific cases, such as when a person is dissatisfied with a decision of the Identification and Registration Committee (which is established to adjudicate over matters arising and or related to registration under Section 83(1) (a) of the Act), Section 83(2) allows for an appeal to be made to the High Court.

Identity theft

In addition to Sections 76, 77 and 78 of the ROPA, which outline several offences related to identity theft and related crimes, the DPPA also makes provisions for the protection of personal data.

The country also has a National Cyber Security Framework[124] as well as cyber

123 Section 29.

124 Global Cyber Security Capacity Centre, Cybersecurity Capacity Review of the Republic of Uganda, (Oxford: United Kingdom, 2016), accessed July 28, 2021, *https://www.nita.go.ug/sites/default/files/publications/Uganda%20CMM.pdf*

laws[125] for prosecuting and preventing cyber crimes, including the National Information Technology Authority, Uganda Act, 2009, the Computer Misuse Act, 2011, the Electronic Signatures Act 2011, the Regulation of Interception of Communications Act, 2010 and, the Uganda Communications Act, 2013.

These laws work together to regulate and prohibit identity crimes. By mandating SIM registration and identity verification, it is possible for agencies such as NITA-U to connect a person to certain activities performed through their online identity and to prosecute them.

125 Unwanted Witness and Civil Rights Defenders, Analysed Cyber Laws of Uganda, (Kampala: Uganda, 2016), accessed July 28, 2021, *https://www.unwantedwitness.org/download/uploads/Analysed-cyber-laws-of-Uganda.pdf*

CONCLUSION

Although being able to own and present legal means of identification is important, especially for government planning and budgeting purposes, the registration process currently in place in Uganda through the ROPA works to exclude many, particularly the elderly and members of minority groups and communities. These exclusions reflect a lack of attention during the preliminary evaluation and implementation stages to engage stakeholders from these marginalised groups. They also point to inefficiencies in the scoping and environmental scan conducted prior to launching the project.

The absence of safeguards against mission creep and data breaches in the enabling statute, the ROPA, as well as staffing issues in the NIRA plague the registration exercise. This gives rise to such issues as authentication errors and inadequate arrangements for the notification of applicants, which increase the difficulty involved in obtaining the mandatory cards.

The following recommendations could work towards creating a digital ID system grounded in equity, inclusion, and social justice.

Civil society

Awareness raising and advocacy

Due to their proximity to members of the public, civil society organisations such as Unwanted Witness have the opportunity to pinpoint pressure points in the rollout of the national digital ID project. Organisations such as Unwanted Witness have championed the causes of the marginalised in the deployment and integration of the system through press releases, interviews, reports and by instituting court action against the government when necessary. These activities are commendable and should be fostered.

Government

Public consultation and research

To address the issues raised above and create an equitable national digital ID system, the Ugandan government needs to engage extensively with stakeholders across the board to develop inclusive measures so that all Ugandan citizens will be able to benefit from it. This can be achieved through public consultation and ongoing research on service design to understand how well the digital ID systems meets the needs of the population. For example, the ID should not be mandatory to receive public services such as vaccinations or similar benefits.

Public sensitisation and education on digital hygiene

There is a major lack of awareness building activities carried out by the government to educate people on the need for the national ID, and how to protect this information once procured. This puts people at risk of their information being stolen and misused, for example, NIN numbers can be used by criminals to register their SIM cards. Lost and stolen IDs may also be used by criminals to carry out transactions or sign contracts. There is a general lack of awareness among the population on how to protect their NINs from being exposed to third parties. Governments should run sensitisation campaigns to educate the public on the role of the ID and the importance of keeping their personal information safe.

Transparency

The government should promote transparency around the entire ID programme by making public the future scope and any planned uses of the IDs, by ensuring that the DPPA is enforced and is disclosing any data breaches, and by conducting ongoing monitoring on how the digital ID system may be compromised or abused by cybercriminals and similar operations.

In developing policies, policymakers should work hand-in-hand with civil society groups and implement their recommendations. Policymakers should also be more circumspect and less hasty in the deployment of policies. By conducting surveys and listening to the various perspectives of members of the public, policymakers will be able to make well-grounded decisions for the general benefit of all. Policymakers should also work with predetermined standards in the procurement of services and consultants to avoid bias and inefficiency.

Technologists and private sector players

Building responsible technology

Like policymakers, technologists need to work with codes of standards to develop beneficial, responsible technology. In today's digital society, it is extremely important for engineers and developers to work deliberately to implement and incorporate data protection and privacy guidelines into their code and products. Furthermore, more transparency and explainability ought to be provided into the workings of the ID project. At present, it is unclear how much access is given to private and government players who are able to access the database in order to obtain information or conduct security checks for carrying out services.

Further research is needed to identify the real impact of the project on the Ugandan economy and citizenry in order to justify it. It would also be useful for audits to be conducted on the management of the scheme to identify useful markers for efficiency. Also significant would be estimates on what it would take

- in terms of financial and human resources - to fully digitise the system and to identify the full benefits of such an endeavour. Interfacing with relevant civil society organisations and stakeholders will enable the government to ameliorate the hardships faced in acquiring a national ID card.

REFERENCES

Albert, Kikonyogo Douglas. "How to know if your National ID Number is on the voters' register." *Tech Jaja*, 14 August 2019. *https://techjaja.com/know-if-national-id-number-on-voters-register/*

Births and Deaths Registration Act. CAP 309 of 1973. *https://www.parliament.go.ug/cmis/browser?id=ed282ea6-3b20-460e-85bd-1c64ac6db0d9%3B1.0*

Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness. Chased Away and Left to Die; How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons. Kampala: Unwanted Witness, 2021. Accessed 11 June 2021. *https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf*

Committee on Defence and Internal Affairs. Report of the Committee on Defence and Internal Affairs on the Inquiry into the Procurement of Equipment for the National Security Information System Project (NSIS)/the National ID Project. Kampala: Parliament of Uganda, 2012. Accessed 26 July 2021. *https://www.parliament.go.ug/cmis/browser?id=7c240510-4fe3-4f58-9758-d1b6e06876fe%3B1.0.*

Daily Monitor. "2.4 million Ugandans don't have national IDs." 6 February 2019. *https://www.monitor.co.ug/News/National/2-4-million-Ugandans-don-t-have-national-IDs/688334-4970294-ohwoha/index.html.*

Daily Monitor. "National ID errors make elderly miss SAGE cash," 11 July 2020. *https://www.monitor.co.ug/uganda/special-reports/national-id-errors-make-elderly-miss-sage-cash-1899228.*

Data Protection and Privacy Act, No. 9 of 2019. *https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf.*

Global Cyber Security Capacity Centre. Cybersecurity Capacity Review of the Republic of Uganda. Oxford: United Kingdom, 2016. Accessed 28 July 2021. *https://www.nita.go.ug/sites/default/files/publications/Uganda%20CMM.pdf.*

Glossary, Thomson Reuters - Practical Law. "Data minimisation." Accessed 27 July 2021, *https://uk.practicallaw.thomsonreuters.com/w-014-9030?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true.*

Habaasa, Gilbert and Jonan Natamba. "Civil registration and national identity system all under one roof: Uganda's fastest path to the revitalization of CRVS for Africa." *Statistical Journal of the IAOS 34*, no. 3 (2018): 453-59. *https://doi.org/10.3233/SJI-180429.*

Hansard Parliamentary Debates (Uganda). 11 March 2020. *https://www.parliament.go.ug/cmis/views/e0bf0740-8668-47dd-b962-9704fea9a47f%253B1.0*

Initiative for Social and Economic Rights and Unwanted Witness. Civil Society Drags Government To Court Over Requirement To Have National ID Card Before Receiving Covid 19 Vaccine. Kampala: Initiative for Social and Economic Rights and Unwanted Witness, 2014. Accessed 27 July 2021. *https://www.iser-uganda.org/images/downloads/COVID19_vaccine_and_IDs-ISER_Press_Briefing.pdf.*

Momodu, Sulaiman. "Uganda stands out in refugees hospitality." *United Nations Africa Renewal*. *https://www.un.org/africarenewal/magazine/december-2018-march-2019/uganda-stands-out-refugees-hospitality.*

Office of the Auditor-General. A Value For Money Audit Report on the identification and registration of persons by the National Identification and Registration Authority (NIRA). Kampala: The Republic of Uganda, 2018. Accessed 29 July 2021. *http://www.oag.go.ug/wp-content/uploads/2019/05/Identification-Registration-of-Persons-NIRA.pdf.*

Okiror, Samuel. "Uganda's ID scheme excludes nearly a third from healthcare, says report," *Guardian*, 9 June 2021. *https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report.*

Privacy International. "How national ID systems make social protection inaccessible to vulnerable populations." *IFEX*. Last modified 12 April 2021. *https://ifex.org/how-national-id-systems-make-social-protection-inaccessible-to-vulnerable-populations/.*

Privacy International. "One Year On, what has Uganda's Data Protection Law Changed?" Last modified 3 March 2020. *https://privacyinternational.org/news-analysis/3385/one-year-what-has-ugandas-data-protection-law-changed*

Registration of Persons Regulations, No 67 of 2015. *http://ugandanlawyer.com/wp-content/uploads/2019/03/Registration-of-persons-regulations-2015.pdf*

Regulation of Interception of Communication Act, No 18 of 2010. *https://chapterfouruganda.org/sites/default/files/downloads/Regulation-of-Interception-of-Communication-Act-2010.pdf*

Regulation of Interception of Communication Act, No 18 of 2010. *https://chapterfouruganda.org/sites/default/files/downloads/Regulation-of-Interception-of-Communication-Act-2010.pdf*

Resilient Africa Network. Understanding the Benefits, Costs, and Challenges of the National: Identification System in Uganda: Findings from a Household Survey and a Costing Study. Kampala: USAID, 2019. Accessed 28 July 2021. *https://www.ranlab.org/wp-content/uploads/2020/10/Understanding-the-Benefits-Costs-and-Challenges-of-the-National-Identification-System-in-Uganda-1.pdf*

The Anti-Terrorism Act, 2002. *http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf*

The Constitution of the Republic of Uganda, 1995. *https://www.parliament.go.ug/cmis/views/e138fbaf-95f5-4cbc-ac33-b4678be3577a%253B1.0*

The Data Protection and Privacy Regulations, 2021. Statutory Instrument 21 of 2021. *https://www.dataguidance.com/sites/default/files/uganda_data_protection_regulations_small.pdf*.

The Independent. "Police building technology interface with NIRA to access data." 16 March 2021. *https://www.independent.co.ug/police-building-technology-interface-with-nira-to-access-data/*.

The National Information Technology Authority, Uganda Act, No 4 of 2009. *https://www.nita.go.ug/sites/default/files/publications/NITA-U%20Act%20%28Act%20No.%204%20of%202009%29.pdf*.

The Refugees Act, No 21 of 2006. *https://www.refworld.org/pdfid/4b7baba52.pdf*.

The Registration of Persons Act. No. 4 of 2015. *https://www.ict.go.ug/wp-content/uploads/2018/06/Registration-of-Person-Act-2015.pdf*

Unwanted Witness and Civil Rights Defenders. Analysed Cyber Laws of Uganda. Kampala: Uganda, 2016. Accessed 28 July 2021. *https://www.unwantedwitness.org/download/uploads/Analysed-cyber-laws-of-Uganda.pdf*

Unwanted Witness, Uganda's Digital Identification Systems and Processes In a Protracted Crisis: What Can Be Done? Kampala: Unwanted Witness, 2020. Accessed 19 May 2021, *https://www.unwantedwitness.org/download/uploads/Ugandas-Digital-Identification-Systems-and-Processes-in-a-protracted-crisis.pdf*.

Unwanted Witness. "Sharing of the national identity card database with private telecoms is prone to abuse/misuse." Accessed 28 July 2021. *https://www.unwantedwitness.org/sharing-of-the-national-identity-card-database-with-private-telecoms-is-prone-to-abusemisuse/*.

Unwanted Witness. "Sharing of the national identity card database with private telecoms is prone to abuse/misuse." Accessed 28 July 2021. *https://www.unwantedwitness.org/sharing-of-the-national-identity-card-database-with-private-telecoms-is-prone-to-abusemisuse/*.

Unwanted Witness. "Unwanted Witness Condemns the criminal use of citizens' bio data & calls on gov't to formulate safeguards to protect lives and property." Accessed 28 July 2021. *https://www.unwantedwitness.org/unwanted-witness-condemns-the-criminal-use-of-citizens-bio-data-calls-on-govt-to-formulate-safeguards-to-protect-lives-and-property/*.

Unwanted Witness. "Unwanted Witness Condemns the criminal use of citizens' bio data & calls on gov't to formulate safeguards to protect lives and property." Accessed 28 July 2021. *https://www.unwantedwitness.org/unwanted-witness-condemns-the-criminal-use-of-citizens-bio-data-calls-on-govt-to-formulate-safeguards-to-protect-lives-and-property/*.

Unwanted Witness. Data Protection and Privacy Law Analysis. Kampala: Unwanted Witness, 2019. Accessed 27 July 2021. *https://www.unwantedwitness.org/download/uploads/Data-Protection-and-Privacy-Law-Analysis.pdf*

Unwanted Witness. Uganda's Digital ID System: A cocktail of Discrimination. Kampala: Unwanted Witness, 2020. Accessed 19 May 2021. *https://www.unwantedwitness.org/download/uploads/UgandaE28099s-Digital-ID-System.pdf*.

World Bank Group. Digital Identity Toolkit: A Guide For Stakeholders In Africa. Washington DC: World Bank Group, 2014. Accessed 26 July 2021. *https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y*.

World Bank Group. The State of Identification Systems In Africa: Country Briefs. Washington DC: International Bank for Reconstruction and Development/The World Bank, 2017. Accessed 7 October 2017, *https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y*.

World Bank. ID4D Country Diagnostic: Uganda. Washington DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 2018). Accessed 19 May 2021, *http://documents1.worldbank.org/curated/en/921761542144309171/pdf/132011-REVISED-PUBLIC-ID4D-Uganda-Diagnostic-12282018.pdf*.

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. ■