Digital Identity in Nigeria

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

RESEARCH & WRITING
Babatunde Okunoye

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 Nigeria

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 Nigeria

By Babatunde Okunoye

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 Nigeria case is one of the ten country case studies RIA and CIS commissioned in this project, and was researched and written by Babatunde Okunoye. 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 Babatunde Okunoye, 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

With the support of international partners such as the World Bank, the French Agency for Development and the European Investment Bank, Nigeria commenced its digital identity programme in 2007 with the passage of the National Identity Management Commission (NIMC) Act. The government had enrolled 56 million people by June 2021, with the stated goals including improving security and harmonising existing databases of government ministries, departments, and agencies towards increasing government efficiency. Nevertheless, as with several other digital identity projects in Africa, the implementation of Nigeria's digital identity project has revealed gaps relating to the rights of people who enrol for the digital identity, and whose digital identity data the system administers. Considering potential rights infringements perpetuated by digital identity programmes, this case study uses a Digital ID Evaluation Framework to analyse and determine whether Nigeria's Digital ID programme upholds the rights of enrolees in its implementation. The Evaluation Framework is used to examine digital IDs with rule of law tests, rights-based tests, and risk-based tests before making recommendations for stakeholders.

ACRONYMS AND ABBREVIATIONS

BVN	Bank Verification Number
CAC	Corporate Affairs Commission
CBN	Central Bank of Nigeria
CDS	Chief of Defence Staff
CNII	Critical National Information Infrastructure
DNCR	Department of National Civil Registration
EFCC	Economic and Financial Crimes Commission
e-ID	Electronic Identity
FIRS	Federal Inland Revenue Service
FMI	Federal Ministry of Interior
FRSC	Federal Road Safety Commission
GDP	Gross Domestic Product `
ID	Identity
INEC	Independent National Electoral Commission
IPPIS	Integrated Payroll and Personnel Information System
MNOs	Mobile Network Operators
NDPR	Nigeria Data Protection Regulation
ngCERT	Nigerian Computer Emergency Response Team
NHIS	National Health Insurance Scheme
NIMC	National Identity Management Commission
NIN	National Identity Number
NIS	Nigeria Immigration Service
NITDA	National Information Technology Development Agency `
NPC	National Pension Commission
NPC	National Population Commission
NPF	Nigeria Police Force `
NSA	National Security Adviser
ONSA	Office of the National Security Adviser
QR code	Quick Response code
SSS	State Security Service

UN	United Nations
UNICEF	United Nations Children's Emergency Fund
USSD	Unstructured Supplementary Service Data

CONTENTS

INTRODUCTION

Nigeria, in West Africa, is the most populous country in Africa, with 200 million people (World Bank, 2021). Although Nigeria also has the largest economy on the continent, with Gross Domestic Product (GDP) of US$448 billion (World Bank, 2021), systemic inequality is entrenched and the country has the largest number of people living in extreme poverty globally, having overtaken India as the poverty capital of the world (Slater, 2018).

Nigeria's deep developmental needs have been the focus of international developmental projects, a case in point being the digital identity project carried out with the backing of the World Bank (World Bank, 2020), among other partners. The digital identity project draws inspiration from target 16.9 of the UN Sustainable Development Goals, which is to ''provide universal legal identity: By 2030, provide legal identity for all, including birth registration''. By doing so, it seeks to address the socio-economic exclusion that is foisted on people who lack legal identity. These marginalised individuals are more likely to be women and children, remote and rural residents, the forcibly displaced, ethnic and linguistic minorities, people with disabilities, and those with low connectivity or technical literacy (World Bank, 2021).

Nigeria had systems in place for foundational digital ID prior to the current system (World Bank, 2016). In 1978, the Department of National Civic Registration (DNCR), under the Federal Ministry of Interior (FMI), was given the responsibility to enrol every Nigerian citizen 18 years or older, and issue a national identity card based on biographic data. This programme failed after 18 months. In the early 2000s, the DNCR restarted the failed programme, and contracted a private service provider for the project. This second project focused on issuing identity cards based on barcode technology to citizens and separated databases of female and male residents. The contracted firm, Sagem, completed the enrolment of 52.6 million out of 60 million residents and issued 37.3 million identity cards. The cost to the federal government was approximately USD 236.8 million. This second digital identity project was also shelved in 2006, amid allegations of financial inducements (Ohia, 2012) offered to government officials by the contractor in order to win the contract. The abrupt end to the project caused by conflicts between the National Identity Management Commission (NIMC) and Sagem, stemming from disagreements on the financial terms of the contract resulted in the non-fulfilment of contract deliverables, such as 60 million ID registrations and ID cards (National Identity Management Commission, 2001). An important bottleneck arising from this project, which also led to its non-completion, was the lack of transfer of technical know-how on the operation of the ID system; only Sagem staff could operate the system. Lessons learnt from this

failed project led the NIMC to insist on transfer of expertise from international technical partners to NIMC staff in the current digital identity project (Centre for Internet and Society, 2021).

Nigeria's current attempt at a digital identity scheme is its third and began in 2007. It commenced with the passage of the National Identity Management Commission (NIMC) Act (National Identity Management Commission, 2007), thus laying a legislative foundation for the digital identity project. The National Identity Management Commission (NIMC) replaced the Department of National Civil Registration (DNCR). The current attempt at digital identity separated the objective of creating a unique national identification scheme from card issuance and provision of electronic verification services (World Bank, 2016).

METHODOLOGY

The data informing this case study was obtained through participant observation, desk research and expert interviews. The researcher employed participant observation during enrolment in Nigeria's ID programme in Abuja, Nigeria's political and administrative capital, in March 2015, and during the process of updating his digital identity information in Lagos, Nigeria's commercial capital, in October 2020. Desk-based research was done on published reports by entities connected with the digital identity programme, such as the World Bank and the NIMC Desk-based research also involved a review of live casts conducted by organisations with thought leadership on digital identity systems in Africa, such as ID4Africa and the Centre for Internet and Society. Informal interviews were conducted with NIMC staff at enrolment centres and with members of civil society in Nigeria.

1.1 OVERVIEW OF NIGERIA'S FOUNDATIONAL DIGITAL ID SYSTEM

At the core of Nigeria's foundational digital identity scheme is the National Identity Number (NIN). The NIN is an 11-digital number which is conferred upon capturing of citizens' data, including biometric information (fingerprints), at enrolment centres. Enrolment data is captured in an enrolment form (NIMC, 2021a) which contains a series of questions to establish foundational identity. To be eligible for enrolment, citizens of 16 years and older must present supporting documentation proving their nationality or residency. The NIMC lists a total of 16 different supporting documents individuals can present for enrolment, thus limiting the possibility of exclusion for lack of supporting documentation (National Identity Management Commission, 2021). Individuals below the age of 16 are enrolled as minors. Enrolment for the digital identity is free. It commenced

in February 2012 (World Bank, 2016), and was made mandatory in January 2019 (Vanguard, 2018) as a prerequisite to obtaining public and private services such as international passports, driver's licences and pension plans (Macdonald, Nigeria reiterates crucial role of biometric national ID, updates SIM registration policy, 2021).

One of the stated aims of the NIN is to harmonise other functional identities and databases of government ministries, departments and agencies in operation in the country, such as those dedicated to driver's licences, Bank Verification Numbers (BVN), the National Health Insurance Scheme (NHIS), the Federal Road Safety Commission (FRSC) and the Independent National Electoral Commission (INEC) (National Identity Management Commission, 2015). Upon enrolment, citizens' data is stored in a database operated by the NIMC and is used for verification and authentication of identity in transactions with public and private organisations. The NIMC has a primary database as well as a secondary database (for disaster recovery) and has plans to establish other disaster recovery sites across the country (Centre for Internet and Society, 2021). A smartcard was initially issued alongside the NIN, but its issuance was shelved because it caused the cost of the digital identity project to spiral beyond its budgetary allocation (ID4Africa, 2020). The national digital identity scheme also has a mobile app which confers digital identity that can also be used for verification and authentication (National Identity Management Commission, 2021).

In pursuit of developmental goals, including target 16:9 of the UN Sustainable Development Goals, digital ID programmes have been rapidly implemented across the world. Nevertheless, these programmes have often sped along without a well-considered evaluation about the privacy, surveillance, and exclusion harms of state-issued digital IDs in several parts of the world (Centre for Internet and Society, 2020).

Naturally, there has been a strong push-back by civil society groups who advocate for digital rights, resulting in significant litigation in countries such as the UK, India and Kenya. In light of the privacy, surveillance and exclusion harms inherent to digital ID programmes, the Centre for Internet and Society India developed a digital ID evaluation framework (Centre for Internet and Society, 2020) to determine whether particular digital ID programmes are rights respecting while achieving target 16:9 of the Sustainable Development Goals of providing legal identity for all, including free birth registrations by 2030.

The evaluation framework examines digital IDs with three distinct tests namely: rule of law tests, rights-based tests and risk-based tests, and will be applied in this report to evaluate the digital ID system in Nigeria.

RULE OF LAW TESTS

2.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law?

Nigeria's National Identity Scheme is authorised by the National Identity Management Commission (NIMC) Act of 2007 (National Identity Management Commission, 2007). The Act established the National Identity Management Commission (NIMC) as an agency of the Federal Government of Nigeria, which is responsible for the administration and implementation of the national identity system. The NIMC Act of 2007 was passed by both houses of Nigeria's National Assembly – the House of Representatives and the Senate - on 17 May 2007 and 23 May 2007 respectively. It was assented to by the President on 25 May 2007. Nigeria's ID programme passes the legality test because it is backed by validly enacted legislation.

QUALITY OF LAW

Generally, the NIMC Act of 2007 is sufficiently clear on the conditions and circumstances in which the authorities are empowered to collect and process the personal data of citizens. These conditions and circumstances are contained in the many sections of the law (National Identity Management Commission, 2007). Nevertheless, there is some ambiguity in aspects of its provisions. For example, Sections 26(2) and (3c) state[9] that the NIMC may provide another person with ID information of enrolees without their consent, so long as this provision is authorised by this section – for any purpose specified in a NIMC regulation.

Hence the law includes the possibility, through this section and the passage of a regulation, that personal data of citizens could be transferred to third parties under as yet unclear terms, since we cannot foresee the nature of potential regulations in this regard. The importance of this section is perhaps heightened by Nigeria's Revised National Identity Policy, which mandates the linking of SIM cards to the National Identity Number (NIN) database (Nigerian Communications Commission, 2021). This provision, although clear on the terms of sharing of data

9 26(2): ''Notwithstanding any other provisions of this Act, the Commission may, without a registered individual's consent provide another person with information recorded in the individual's entry in the database if the provision of the information is authorized by this section''. 26(3c): ''The provision of information by this section is authorized by this section where such disclosure is for any purpose as may be specified by the commission in a regulation''.

for crime and national security purposes, is still vague regarding the extent of sharing of citizen's data in other scenarios.

The NIMC Act of 2007 is a 24-page document containing 34 sections. Its implementation through the National Identity Management Commission has brought about largely positive regulatory results in the identity management sector in Nigeria. These include enabling identity checks for security purposes and enabling greater access to public and private services for those who had been denied such access because of a lack of a legal identity (Macdonald, 2021).

CLARITY AND PRECISION OF LAW

As will be seen in the analysis contained in sections of this case study, the NIMC Act of 2007 is largely clear and precise in the description of the mandate of the NIMC and the administration of Nigeria's identity system. It generally avoids vagueness and ambiguity, thus limiting the scope for abuse and the exercise of discretion. Nevertheless, some policy matters regarding collection, storage, use, and sharing of personally identifiable information have been delegated to a rulemaking body that is part of the Executive. An example of this can be seen in Section 26, which allows for digital ID data to be shared without the consent of the data subject, for the purposes of crime detection and national security. Also, as explained in the section above, the law does contain some ambiguity in the sense that it gives room for the passage of (as yet unspecified) regulations by the NIMC, which allows for the sharing of user data with third parties, thus potentially creating the possibility for abuse.

2.2 LEGITIMATE AIM

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

The purpose of the NIMC Act of 2007 is specified in Section 5 of the law, and it states that the NIMC shall be used for 16 purposes, which include:

> (a) *"Create, manage, maintain and operate the National identity database established under section 14 of this Act including the harmonization and integration of existing identification databases in government agencies and integrating them into the national identity database.*
>
> (b) *Carry out the registration of citizens of Nigeria into the national identity database.*
>
> (c) *Carry out the registration of non-citizens of Nigeria who are lawfully resident in*

> *Nigeria.*
>
> (d) *Issue a general multi-purpose identity card to any person registered pursuant to paragraphs (b) and (c) of this section.*
>
> (e) *Collate information obtained by the Commission in pursuance of its functions under this Act and reproducing such information as may be required, from time to time."*

Taken together, the long title of the NIMC Act (*An Act to provide for the establishment of a national identity database and the national identity management commission charge with the responsibilities for the maintenance of the national database, the registration of individuals, and the issuance of general multipurpose identity cards; and for related matters*), Section 5 of the NIMC Act 2007, and the vision of the NIMC as stated on its website give an assessment of the aim of the Act and the digital ID. The vision of the NIMC states:

> *It is our vision to provide [a] sustainable world-class identity management solution to affirm identity, enhance governance and service delivery in Nigeria.*

Therefore, we can deduce that the aims of the NIMC, apart from those already mentioned in Section 5 of the NIMC Act and the long title of the Act, include to affirm identity and enhance governance and service delivery in Nigeria.

The aims of the digital ID programme as detailed above do not express meeting social needs, such as national security, public safety or the economic well-being of the country, or its use for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. However, some of these aims seem implied from Section 5 of the NIMC Act.

2.3 DEFINING ACTORS AND PURPOSE

Does the law clearly specify the actors and the purposes that flow from the legitimate aim?

The NIMC Act clearly states the category of actors who can use the foundational digital ID. These actors can be found in the various sections of the legislation. They include:

> (a) Government agencies operating the existing functional identity databases (Section 5a). These agencies are listed in Section 2 as the Independent National Electoral Commission (INEC), the National Health Insurance Scheme (NHIS), the Federal Road Safety Commission (FRSC), the

Federal Inland Revenue Service (FIRS), the National Pension Commission (NPC), the Nigeria Police Force (NPF), the Nigeria Immigration Service (NIS), the Office of the National Security Adviser (ONSA), the National Population Commission (NPC), the Central Bank of Nigeria (CBN), the State Security Service (SSS), the Economic and Financial Crime Commission (EFCC), the Chief of Defence Staff (CDS) and the Corporate Affairs Commission (CAC).

(b) The Judiciary (Section 15a).

(c) Any person or corporate body under conditions as specified in Section 26 of the law, with the authority of the commission and consent of the data subject. However, under Section 26, digital ID data can be shared by the NIMC without the consent of the data subject for purposes of national security, crime detection, and any purpose specified by the NIMC in a regulation. An example of the sharing of digital ID data by the NIMC with third parties in Nigeria is the sharing of data with VerifyMe, a private firm offering digital identity and verification services to a wide range of industries and the retail market (VerifyMe, 2021).

(d) The owner of the digital ID.

The Access to Register Information in the National Identity Database Regulations 2017 (National Identity Management Commission, 2017), governed by the NIMC Act, give more clarity on who can use the digital ID. Sections 5 to 8 of the regulations have provisions and rules for the use of digital ID by security agencies, government agencies and registered private entities. Not everyone agrees that private companies should be interacting with the national identity database. Perhaps the most prominent critics of this arrangement have been civil society.

Objecting to this sharing of citizens' data, Boye Adegoke, Senior Programme Manager, Paradigm Initiative, a civil society organisation in Nigeria noted for digital rights advocacy stated, "Reducing personal details of individuals shared with either the CBN, the NIMC or the Immigration Services to elements of business transactions is very worrying and clearly violates privacy laws" (Hersey, 2020). Paradigm Initiative had previously challenged the NIMC in court about its mobile USSD-enabled ID service, which revealed the NIN of Nigerians to anyone who had their surname and date of birth information (Andersen, 2019).

The purposes or the category of purposes for which the digital ID is used is backed by law, but is not always clearly and explicitly defined, as seen in the sections above. The agencies and individuals who have access to the digital ID are clearly defined, but less clearly defined is the nature of data required to fulfil this legitimate aim of the proposed use, in order to limit the collection and retention of

data to that which is strictly necessary. Nigeria has a Data Protection Bill (Nigerian Communications Commission, 2020) which brings some clarity to data privacy in Nigeria. When passed into law, it will contribute to tidying up the legal framework around the protection of citizens' data.

2.4 REDRESSAL MECHANISMS

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

An express provision for user notification in case of use of their ID in authentication, or in breaches or violations, is not mentioned in the NIMC Act. However, the possibility of user notification is provided for in Section 26 of the Act, which deals with disclosure of registered information. Section 26(1a,b)[10] of the NIMC Act states that no person or corporate body shall have access to ID database information except with the authorisation of the NIMC, or with the authority or consent of the person. Additionally, the NIMC mobile app notifies users when their identity has been verified and lets them know who verified them, when, and the type of verification (National Identity Management Commission, 2021).

However, the Data Protection Bill of 2020 (Nigerian Communications Commission, 2020) has provisions for user notification. In Section 17 (3) it states unequivocally that ''a data subject has the right to be notified of the data breach affecting him or her within 48 hours after notification to the Commission'' and Section 17(4)[11] further clarifies that the details of this notification must include the nature of the personal data breach, contact details of the data protection officer, consequences of the breach, and measures taken by the data controller in

10 26 (1) No person or body corporate shall have access to the data or information contained in the database with respect to a registered individual entry except with the authorization of the commission and only if:

(a) An application for the provision of the information of that person is made by or with the authority of that individual; or

(b) the individual otherwise consents to the provision of that information to that person."

11 17(4) The notification referred to in subsection (3) shall — (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

response to the breach.

Although not stated explicitly in the Data Protection Bill, the measures which might be taken to mitigate possible adverse effects of a data breach will include cybersecurity incident management, and also law enforcement investigations. It is expected that the Data Protection Bill will be passed into law (Centre for Internet and Society, 2021), and together with the Cybercrime Act and Cybersecurity Policy (Office of the National Security Adviser, 2021) should provide adequate policy cover for data protection in Nigeria.

Section 26(1) of the NIMC Act confers individuals with the right to access their personally identifiable information collected through the use of digital ID. The right to be able to confirm the data being held by the data controller (the NIMC) and to be able to obtain a copy of the same is not explicitly mentioned but should derive from the right to access the information from Section 26(1). Section 3 of the Access to Registered Information in the National Identity Database Regulations 2017 (National Identity Management Commission, 2017) allows users access to their personal information. Section 18 of the Data Protection Bill also provides provisions for data subjects to access their data.

The right of an individual to seek corrections and/or amendments to information where it is inaccurate is recorded in Section 22 of the NIMC Act titled ''Changes of circumstances and errors''. The NIMC Act does not have provisions for deletion. Section 20 of the Data Protection Bill 2020 titled ''Right to rectification, erasure, and restitution of processing'' makes provision for the deletion of data where it states in Section 20(1)[12] that the data subject has the right to the rectification, blockage or erasure of false or unlawfully processed data.

Section 31d (6) of the NIMC Act suggests the powers of the NIMC to confirm the data being held by the data controller, only once relevant regulation is passed.

The NIMC Act does not provide for redress for individuals in cases where the provisions of laws governing the digital ID are violated by the NIMC. However, in part VI (Sections 28 – 30) of the law titled ''Offences and Penalties'', penalties are given for individuals and corporate bodies for a range of offences relating to the use or misuse of the digital ID.

However, Section 21 of the Data Protection Bill titled ''Right to Judicial Remedy'' states in Section 21(1) that where the provisions of this Act are violated, the data subject shall have the right to a judicial remedy under this Act. Part IV (Sections 44 – 50) of the Data Protection Bill 2020 lists in detail the offences and penalties related to data controllers and processors. Hence, although there are no avenues

12 The data subject shall have the right to the rectification, blockage, or erasure of inaccurate, false or unlawfully processed personal data without delay and free of charge from the data controller.

for redress provided for by the digital ID law itself, Nigeria's Data Protection Bill does make some provision in this regard.

2.5 ACCOUNTABILITY

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

The NIMC Act provides for systems of accountability for some of the bodies which implement and operate the digital ID. This system of accountability only institutes penalties for offences perpetuated by individuals and corporate bodies which use the digital ID, including offences such as unlawful access to information in the database and refusal to give relevant data and information to the NIMC. This system of accountability is found in part IV (Sections 28 – 30) of the NIMC Act, titled ''Offences and Penalties'', and accountability typically takes the form of imprisonment and fines.

However, it must be stated that no system of accountability is prescribed for the NIMC itself, which is the administrator. Furthermore, accountability for private actors is not enough, particularly because Nigeria does not at present have a data protection law or a data protection commission. The Data Protection Bill, in Section 7, makes provision for the creation of a data protection commission that has oversight over all data controllers and processors within the country. According to Section 64 of the Data Protection Bill, ''the Federal High Court has exclusive jurisdiction over all matters, suits and cases arising out of or pursuant to or consequent upon the Data Protection Bill 2020 Act or its subsidiary legislation''. All stakeholders hope it will be passed soon (Okonji, 2019). It is also not clear if the exemption from offences and penalties for the NIMC extends to its partner agencies (as enumerated above) listed in Section 2 of the NIMC Act. While there are no systems of accountability in the NIMC Act for the NIMC itself, one must look to relevant regulations such as the Nigeria Data Protection Regulation (NDPR) (National Information Technology Development Agency, 2019), which institutes some form of accountability and oversight mechanism over relevant actors in the digital ID ecosystem, including the NIMC. The NDPR achieves this through its provisions, such as in part 3, which mandates annual data protection audits by organisations that handle citizens' data to the National Institute for Information Technology Development Agency (NITDA).

The accountability systems governing Nigeria's digital ID programme do not constitute an effective regulatory framework, do not provide a proper delineation of responsibility among the various actors in the digital ID system, lack sufficient transparency, make no provision for user breach notification, and have no efficient grievance redress procedures. The NIMC Act does not separate the

role of the NIMC as the administrator in charge of the storage of personal data; and its role as a regulator, which licenses other agencies to perform enrolment and authentication functions as well as being in charge of grievance redress of the digital ID programme. These roles all seem to be played by the NIMC, which can result in conflicts of interest and abuses of regulatory powers. It is thus important that the Data Protection Bill 2020 is passed into law, and a National Data Protection Commission instituted according to Section 7 of the Bill. The Data Protection Act will enhance the regulatory framework governing identity data, for instance by the Data Protection Commission which takes over the role of regulator from the NIMC in terms of the Act.

The accountability systems set over the digital ID ecosystem, as established in the NIMC Act, can be much improved upon. While only applying to individuals and corporate bodies, it places no burden of accountability on the NIMC itself, or its partner agencies. To be fit for purpose, the digital ID system has to address the many concerns expressed above, including instituting accountability mechanisms for the NIMC itself, and separating the roles of administrator and regulator – both roles being played by the NIMC at the moment.

2.6 MISSION CREEP

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital ID?

The NIMC Act provides legislative and judicial oversight mechanisms to deal with cases of mission creep in the use of digital IDs. Mission creep is checked by the NIMC stipulating the nature of data to be included in the identity database (Section 17 of the NIMC Act) and by stating the purpose of the data to be collected (Section 15 of the NIMC Act).

A copy of the current digital ID enrolment form, with a number of these information fields, can be found on the NIMC website (National Identity Management Commission, 2021).

The NIMC also has a privacy and security policy that aims to limit technological access to the system, which, in turn, limits mission creep. The NIMC has a regulation on ''Access to Register information on the National Identity Database'' that regulates the sharing of information on the database with actors in government, security agencies and the private sector. Under this regulation, access is granted to these institutions after the submission of a written request to the NIMC by senior leadership of the institutions. Further details on how this regulation is administered can be found below in the ''Access control'' section under the heading ''Rights-based tests''.

RIGHTS-BASED TESTS

3.1 NECESSITY AND PROPORTIONALITY

Are the privacy violations arising from the use of Digital ID necessary and proportionate to achieve the legitimate aim?

The violations of the right to privacy embedded within Nigeria's digital ID are not proportional to the benefits to be derived from the ID, and neither are they just, fair and reasonable. The most reported violation in the news was the NIMC's mobile USSD service, which allowed anyone with the surname and date of birth of people enrolled in the identity database to access their NIN information. Following lengthy litigation in the Federal High Court Nigeria brought by civil society, the NIMC rectified this problem (Andersen, 2019). Other violations to the right to privacy embedded within Nigeria's digital ID system took place during various parts of the project. These include:

(a) Compulsory enrolment: Enrolment for Nigeria's digital ID scheme was made compulsory in January 2019 (Awojulugbe, 2018) and is seen by the government as important for Nigeria's aspirations towards a digital economy. Enrolment became a precursor to obtaining other important documentation, such as international passports and voter registration cards as stated in Section 27 of the NIMC Act. The requirement of national identity enrolment as a prerequisite for obtaining other public services such as the issuance of international passports potentially excludes individuals without the ID. Enrolment figures reached 56 million by 8 June 2021 (National Identity Management Commission, 2021) out of a total population of 120 million. Enrolment has been hindered by the hesitation of Nigerians who saw no urgency in the need to be enrolled even though enrolment began in 2012. Enrolment has also been hindered by the limited number of enrolment centres available, although the NIMC has worked to increase the number to about 5 000 (Centre for Internet and Society, 2021). It is also likely that enrolment has stalled because of the negative perception of the human rights record of the Nigerian government in recent years. As seen by the public backlash and lawsuit (Macdonald, Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit, 2021) against the updated national ID policy, which mandates that people link their NIN to their SIM cards, many Nigerians are worried that their data is been collected to empower a possible

government clampdown on rights. This perception has caused delays in the public response to this directive, with the government extending the deadline (Nigerian Communications Commission, 2021) for the sixth time, till 31 October 2021, after the initial announcement in December 2020.

(b) Centralised storage and retention: The digital ID system in Nigeria has a centralised retention and storage mechanism for personal information (ID4Africa, 2020). This centralised system creates a huge data privacy and cybersecurity risk, in the absence of a data protection law and national data protection commissioner. Provisions in the NIMC Act prescribing penalties for illegal data access, the NIMC's privacy and security policy (National Identity Management Commission, 2017) and its regulation on ''Access to Register Information on the National Identity Database'' (National Identity Management Commission, 2017) are not sufficient to replace a substantive data privacy law and the office of a national data commissioner. It is important that legislative oversight for the digital identity project is provided by the nation's lawmakers, and not by the NIMC, which administers the ID. The data privacy and cybersecurity risks of a centralised database are mitigated by the existence of primary and secondary databases for disaster recovery (Centre for Internet and Society, 2021).

(c) Procedural safeguards: Some system of accountability is found in part IV (Sections 28 – 30) of the NIMC Act, which tries to establish safeguards against the unlawful use of the digital ID. Provisions in the NIMC Act prescribing penalties for illegal data access, the NIMC's privacy and security policy and its regulation on ''Access to Register Information on the National Identity Database'' also attempt to establish procedural safeguards for purpose limitation, although they alone are not sufficient in the absence of a data privacy law. Identity databases are susceptible to privacy violations without a strong data protection framework in operation.

Nigeria's ID system is necessary, based on the needs and interests of the country. It has been touted by the government as a means to improve security in parts of the country, although that claim has been contested (Adepetun, 2021), and to cut government public expenditure - for example eliminating duplicate payments (ghost workers) in government payrolls. In 2016 the federal government removed over 23 000 ghost workers from its payroll by using a combination of the Bank Verification Number (a functional identity currently being linked with the foundational NIN) and the Integrated Payroll and Personnel Information System (IPPIS) (Premium Times, 2016). The foundational NIN itself has been useful in uncovering discrepancies in the reported dates of birth of

public servants who declared false dates of birth in a bid to illegally prolong their years in service (Centre for Internet and Society, 2021). Nevertheless, despite its seeming advantages, the privacy risks associated with the management of digital identity have to be managed and mitigated.

A framework for answering the proportionality enquiry is by examining if there is:

(i) a 'legitimate goal' or proper purpose;

(ii) 'suitability', namely that the law must be a suitable means of furthering the aforesaid legitimate goal;

(iii) 'necessity', i.e. there must not be any less restrictive but equally effective alternative present; and

(iv) 'balancing', since the measure must not have a disproportionate impact on the rights holder.

In response to the above, specifically answering the proportionality question, the NIMC Act presents a legitimate goal and proper purpose for the ID because it attempts to harmonise the various existing functional identities (Section 5 of the NIMC Act) used by Nigerians and reduces the need to carry multiple identity cards.

Answering the suitability question, the NIMC law is a suitable means of achieving or furthering the aforesaid legitimate goal. Nevertheless, the significant limitations in its provisions (many already discussed in previous sections of this case study), which undermine privacy, encourage mission creep and absolve the NIMC of accountability in the administration of registrant's data, need to be addressed.

Answering the necessity question, there are currently less restrictive but equally effective alternative foundational ID systems present in Nigeria, which could be used in lieu of the existing national identity system. For example, birth certificates and social registers can be tapped into as alternative means of establishing foundational identity. An alternative strategy of government could be to allow individuals who possess such alternative foundational IDs to use them, to avoid them being cut off from services which require foundational IDs as prerequisites for access, while still encouraging enrolment in the digital ID programme, given that many births in Africa are unregistered so many lack valid birth certificates. In 2019 UNICEF, the United Nations Agency for children reported that 17 million (1 in 5) children under the age of five in Nigeria were unregistered or ''invisible'' (UNICEF, 2019).

Answering the balancing question, at the moment, the digital identity scheme does not have a disproportionate impact on the rights holder, although there

are early concerns brought about by the compulsory enrolment which bars individuals from accessing government services unless they have registered for the digital ID.

3.2 DATA MINIMISATION

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

The Nigerian digital ID system does not comply with the principles of data minimisation, as is reflected in several aspects of its design.

First, a core principle of data minimisation is that only the data which is required is collected. As described above, the amount of data collected during registration is far greater than what is required to establish foundational identity. The amount of data collected creates the possibility that it might be used for other, supplementary purposes, rather than those originally intended.

Another principle of data minimisation is that data collected is processed only for legitimate purposes. The NIMC Act specifies the actors who can access data and for what purposes. Nevertheless, the law contains vague provisions, which create potential avenues through which abuses can be perpetrated. For example, under Section 26, digital ID data can be shared by the NIMC with another individual or organisation without the consent of the data subject for purposes of national security, crime detection, and any purpose specified by the NIMC in a regulation. Although there is a policy on privacy and security (National Identity Management Commission, 2017), and regulations on access to registered information in the national identity database (National Identity Management Commission, 2017), the vague wording of Section 26 still opens the door to potential data abuses. Importantly, the Regulation on Access to Registered Information in the National Identity Database in Section 4(b) allows the possibility that access to digital ID data can be granted to third parties, and the individual's consent is deemed to have been given having participated in the digital ID registration exercise, a reality which many ID holders might be unaware of. In addition to the NIMC Act, these published policies also govern the use of digital identity in Nigeria.

Finally, in data minimisation, it is critical that data is stored for only as long as necessary. The NIMC Act does not specify a time limit for which data can be kept, and there is no provision for deletion of data. The planned but not yet implemented Section 20 of the Data Protection Bill and Section 3.1(13) of the Nigerian Data Protection Regulation make provisions for erasure of data in the care of a data controller.

3.3 ACCESS CONTROL

Are there protections in place to limit access to the digital trail of personally identifiable information created through the use of digital ID by both state and private actors?

The NIMC Act does not provide sufficient protections to limit access to digital trails of personally identifiable information. This is consistent with the inadequate data protection provisions already discussed in other sections of this case study.

Section 26 of the law permits private and governmental access to sensitive and personal information attached to the digital ID. Government actors seem to be favoured in accessing the database ahead of private actors, who are required to pay fees to access the data, according to Section 7 of the Regulation on Access to Registered Information in the National Identity Database. Personal data is stored in a centralised or federated database, without a specified time period of retention. The NIMC is in the process of linking the digital ID database to multiple state databases (ID4Africa, 2020), although there does not seem to be a plan yet to link the digital ID database to private databases. The NIMC Act and Access to Registered Information in the National Identity Database Regulation both clarify and provide rules governing whether sharing of digital ID personal data (relating to the authentication transactions) among various agencies is permitted. They are, however, silent on what happens with metadata (relating to the authentication transactions).

The Access to Register Information in the National Identity Database Regulation 2017 implements some form of access control and recording of data flows from the database. Some of these access controls include:

- Excluding biometric information from the list of information which can be accessed from the database (Section 4.2)
- The platforms used to access data are password login-protected, have user accounts, access level rights, login credentials for proper auditing and have further security features in accordance with international best practices (Sections 5 – 7)
- Access is only granted by request of senior leadership of relevant agencies (Sections 5 -7)

3.4 EXCLUSIONS

Are there adequate mechanisms to ensure that the adoption of digital ID does not lead to exclusion or restriction of access to entitlements or services?

The NIMC Act does not make provision for adequate mechanisms to address exclusion from the system. Indeed, exclusion is codified in the law itself, with possession of the digital ID being necessary for accessing a range of government services, such as the issuance of passports, opening of bank accounts, and purchasing insurance policies and health insurance (Section 27, NIMC Act).

These mandatory uses of the digital ID came into force in January 2019. This policy has resulted in a rush on digital identity enrolment centres (Adepetun, NIMC registers 3 million NINs in two months, 2021).

Acknowledging the reliance of the digital ID enrolment and verification process on the availability of Internet connectivity, the NIMC is in the process of facilitating offline and localised verification of the demographic or biometric identity using the QR codes embedded in the new Digital ID card (ID4Africa, 2020).

The lack of adequate numbers of enrolment centres is another source of exclusion. As of February 2021, 56 million people (in a country of 200 million) had enrolled, using about 1 060 enrolment centres. The NIMC is now in the process of including the country's mobile network operators (MNOs) and partner agencies to reach the 9 000 extra enrolment centres required (Okere, 2019)to ensure more inclusive coverage.

An emerging source of exclusion is the spiralling cost of the digital ID project in Nigeria, which has resulted in the NIMC temporarily stopping the issuance of the digital ID card which comes with enrolment. The cost of the card increases the overall cost of the project beyond budgetary allocations. Instead, the digital ID project will, at the moment, focus on the issuance of National Identity Numbers (NIN), in order to reach more citizens (ID4Africa, 2020). At the moment the benefits of the digital ID can still be accessed via the NIN slip and the mobile app.

The NIMC Act does not provide for a grievance redress mechanism, following the principles of natural justice, where the aggrieved digital ID holder (who has experienced authentication failure) is given a right to be heard.

3.5 MANDATORY USE

In case enrolment and use of digital ID are made mandatory, are there any valid legal grounds for doing so?

Registration into the digital ID scheme is mandatory for individuals who intend to access essential public and private services which require the possession of the ID. The NIMC Act made the use of the digital ID for accessing a number of important public and private sector services, such as the issuance of passports and the opening of bank accounts (Section 27), compulsory for all from January 2019. There is no provision for dealing with multiple forms of identities, nor is there an opt-out mechanism where the individual retains their access to the service provided they produce an alternative form of ID. Some state governments, too, have begun requesting the digital ID as a prerequisite to receiving social services (Macdonald, Biometric Update, 2021). In other words, enrolment is *de facto* mandatory because it is difficult to access essential services without the ID. This situation has elicited conversations within civil society uncomfortable with its implications for the country (Proshare, 2020).

RISK-BASED TESTS

4.1 RISK ASSESSMENT

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

The NIMC conducted a risk assessment on privacy, through a call for proposals issued before the implementation of the digital identity project (National Identity Management Commission, 2007). The risk assessment covered a number of important risk factors, such as the need for third party consent, concerns about the use of personal information, and the potential multipurpose uses of the database. Feedback from the privacy impact assessment conducted by research organisations contracted by the NIMC, influenced the NIMC's choices about the design of the digital ID system and its regulations. This feedback provided recommendations for registration procedures and activities, information access and processing, ensuring the security of personal information, and for national identity card issuance and collection, among other recommendations. The Privacy Impact Assessment Report can be accessed on the website of the NIMC (National Identity Management Commission, 2017). The report, in Section 6.1.2, envisaged that Nigerians might be unwilling to participate in the ID enrolment process and recommended, in Section 7.1, an awareness and enlightenment campaign to increase uptake.

The Privacy Impact Assessment Report did not, however, include a risk assessment on exclusion. Nevertheless, in mentioning the mandatory use of the digital ID for exercises such as voting (Section 5), it raises the possibility that those without the ID might be excluded from services for which possession of the digital ID is a mandatory requirement. Additionally, the Privacy Impact Assessment Report does not include a risk assessment on discrimination. However, among its findings in Sections 4.1.3 and 4.1.4 it does mention the fears harboured by people surveyed about the potential sharing and misuse of their personal information by third parties. These were addressed in Section 7.3, which contains recommendations specifically to allay these fears, including the recommendation to limit the access of security agencies to the database, and also limiting their use of the data collected. These recommendations are reflected in some of the NIMC policies already discussed in this case study.

4.2 PROPORTIONALITY

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

The governance of the digital identity scheme in Nigeria demonstrates consideration for the severity of the possible risk of inaccurate data. This is reflected in Section 22 of the NIMC Act titled ''Change of circumstances and errors'', which envisages the possibility of error in recorded data, and which offers the procedure for correcting such errors. The NIMC Act does not, however, envisage or provide redress in scenarios where authentication is rejected or service denied because of inaccurate data.

The governance of the digital ID reflects consideration of the severity of the possible risk of authentication errors. The law connects the identity of the individual to a unique 11-digit NIN, and does not limit identity to a biometric identifier. Thus, multiple enrolments are not possible, because the database automatically detects the registration details from previous enrolment. The NIMC Act does not provide redress in scenarios where authentication is rejected or service denied because of inaccurate data.

Nevertheless, there is an awareness that the authentication process might fail because of a lack of Internet access, on which it is dependent. The NIMC is in the process of enabling authentication and verification through QR codes on the smart digital ID cards in areas with poor or no Internet connectivity. Moreover, on the mobile ID (National Identity Management Commission, 2021), an Internet connection is not required for the verification of a user's ID, although it is needed to verify the identity of others.

The governance of the digital ID does not reflect consideration for the severity of the possible risk of mission creep. Section 26 of the NIMC Act envisages that digital ID data can be shared without the consent of the data subject for purposes of national security, crime detection, and any purpose specified by the NIMC in a regulation. The law does not limit the purposes for which the ID can be used.

Similarly, the NIMC's 'Regulation on Access to Registered Information in the National Identity Database' (National Identity Management Commission, 2017) in Section 4(b) opens the possibility that access to digital ID data can be granted to third parties, and the individual's consent is deemed to have been given having participated in the digital ID registration exercise. This detail might not be known to the millions of people who have already enrolled. The NIMC Act and its regulations do not have enforcement mechanisms for third parties who process data unlawfully. This role is performed by the National Information Technology and Development Agency (NITDA), which has a regulation, the Nigeria Data Protection Regulation 2019 (NDPR) (National Information Technology

Development Agency, 2019) that seeks to secure the rights of data subjects in Nigeria. Nigeria's Draft Data Protection Bill 2020 (Nigerian Communications Commission, 2020) also has provisions for data privacy. The penalties stipulated in the NIMC Act are for individuals who illegally access the digital ID database, are specified in Section 28 of the Act, and include fines and imprisonment.

The NIMC Act does not have an independent oversight mechanism for data protection, other than the NIMC Board itself.

The NIMC Act and its regulations have sections governing the sharing of data between the NIMC and government agencies, other public and private agencies. These sections include NIMC Act Section 26, titled, ''Disclosure of Registered Information'', and Section 4 of the Regulation on Access to Registered Information in the National Identity Database 2017. These provisions define or govern what might constitute indiscriminate data sharing. However, they do not allow for citizens to access information about where their data is going. This role is played by the NIMC on behalf of citizens. The NIMC implements a mechanism to always record flow of data, with time logs, which is considered among the best practises to prevent unauthorised data sharing. For example, Section 8(3) of the Access to Registered Information in the National Identity Database Regulation 2017, titled, ''Rules for providing information to Security and Government Agencies", states: ''The Commission shall keep detailed and accurate records of all instances upon which registered information is released to a security agency or other Government agency''.

The governance of the digital ID reflects consideration of the severity of the possible risk of identity theft. For instance, Section 28 of the NIMC Act governs unauthorised access and specifies penalties for unauthorised access. Also, the Access to Register Information in the National Identity Database Regulation 2017 implements some form of access control and recording of data flows from the database, as detailed under the section on Access control.

Nevertheless, there is no national data protection law (although there is the Nigeria Data Protection Regulation 2019 and a Data Protection Bill 2020) and adequate judicial oversight mechanisms already in place to instil good data collection and storage practices, nor is there a strong, working enforcement system.

4.3 RESPONSE TO RISKS

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

The governance regime provides strategies for dealing with risks. For example, on the National e-ID card, the NIN is embedded on the chip and is not physically

printed on the card (National Identity Management Commission, 2021). The NIN can be retrieved through a USSD code using the phone used to register the NIN. However, the NIN is printed on the National Identity slip. Users of the National Identity mobile app on smartphones (National Identity Management Commission, 2021) who lose their device can simply report it lost, log in from another device and block anyone from using their missing device. Furthermore, Nigeria's cybersecurity policy and strategy makes provisions for incidence management through the Nigerian Computer Emergency Team (ngCERT), established under Section 41c of the Cybercrimes Act of 2015 (Office of the National Security Adviser, 2021). Nigeria's cybersecurity policy also makes room for the protection of Critical National Information Infrastructure (CNII) under the framework of the National Critical Information Infrastructure Protection Unit of the Office of the National Security Adviser (NSA). Digital identity databases are critical infrastructure which fall under Information, Communication, Science and Technology and Public Administration – sectors for CNII protection.

CONCLUSION

The evaluation framework (Centre for Internet and Society, 2020), through its rule of law, rights-based, and risk-based tests, has been used to scrutinise Nigeria's digital ID and we find that although the legislation empowering the digital ID does have provisions which ensure that the digital ID programme respects human rights and minimises risk, it does not go far enough. Several gaps revealed in this case study -such as vaguely worded policies, mandatory enrolment, and the lack of a data protection law and commission - leave room for abuse by those who would seek to use the digital ID to harm human rights and exclude people. It is hoped that this work will lead to a process of stakeholder consultation and dialogue towards possibly closing these loopholes, potentially amending the digital ID legislation and correcting technical implementations which open the door to abuses. To attain this, the following recommendations are offered:

Recommendations for civil society:

- It is important that civil society in Nigeria continue their important work of monitoring and advocating against the rights violations brought about by the digital identity programme, such the litigation against the NIMC's USSD code which revealed the NIN information of Nigerians. The price of freedom is eternal vigilance.
- Civil society should continue their push for the passage of the Data Protection Bill 2020 into law. It is crucial that a national identity project has the legal foundation exemplified by a law passed by the national legislature, rather than a regulation by an agency of government.

Recommendations for policy makers:

- Policy makers are encouraged to pay closer attention to the data privacy concerns around the sharing of digital identity with public and private organisations.
- They are encouraged to expedite the passage of the Data Protection Bill into law.
- The NIMC Act should be amended to institute accountability mechanisms for the NIMC itself, and not just for individuals and corporate organisations who wrongfully use citizens' data.

Recommendations for donor agencies:

- Donor agencies should consider including human rights dialogue, cooperation, monitoring and reporting mechanisms as conditions in development assistance directed towards digital identity programmes. This ensures that the development objective of the donors is not subsumed by the poor human rights standards inherent in some developing country contexts of their grantees.
- Beyond the stated digital ID policies themselves and the actual rollout of the digital identity programme, the broader actions and policies of the government have great importance to the success or failure of the stated aims of the identity project. As seen in this case study, an important objective of Nigeria's digital ID project is to harmonise the data of citizens and residents towards enabling government planning and development. However, there is the perception within the country that human rights standards have dropped in the past few years (Human Rights Watch, 2021), and many feel reluctant to participate in schemes which give more power to the government. For example, although the government had released an updated national identity policy which required individuals to link their NIN to SIM cards in December 2020 (Adepetun, NIMC registers 3 million NINs in two months, 2021), there has been a general hesitation by Nigerians, who see the move as inimical to their interests and wellbeing. The deadline for this NIN-SIM linkage has thus been postponed six times, with the sixth postponement coming in July 2021 (Nigerian Communications Commission, 2021).

The implementation of digital IDs is important within the context of national development plans, and across Africa, their rollout has been supported by international partners such as the World Bank. Nevertheless, the deepening of human rights standards are also important development indices, and cannot be overlooked in the rush to implement digital identity schemes. This is particularly crucial for Africa, where people live under some of the most repressive political contexts in the world. A digital identity project in these contexts should empower citizens while not undermining their rights.

REFERENCES

Adepetun, A. (2021, July 26). Despite security concerns, FG again extends NIN-SIM link deadline by three months. Retrieved from *The Guardian*: *https://guardian.ng/news/despite-security-concerns-fg-again-extends-nin-sim-link-deadline-by-three-months/*

Adepetun, A. (2021, February 8). NIMC registers 3 million NINs in two months. Retrieved from *The Guardian* : *https://guardian.ng/news/nimc-registers-3m-nins-in-two-months/*

Andersen. (2019, August 30). Federal High Court Affirms the Data Privacy Rights of Nigerian Citizens. Retrieved from *Andersen*: *https://ng.andersen.com/federal-high-court-affirms-the-data-privacy-rights-of-nigerian-citizens/*

Awojulugbe, O. (2018, September 19). FG: Mandatory use of national ID number begins in January 2019. Retrieved from *The Cable*: *https://www.thecable.ng/fg-mandatory-use-of-national-id-number-begins-in-january-2019*

Centre for Internet and Society. (2020). Governing ID: A framework for Evaluation of Digital Identity. Retrieved from *Centre for Internet and Society*: *https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity*

Centre for Internet and Society. (2020, March 2). Governing ID: A Framework for Evaluation of Digital Identity. Retrieved from *Centre for Internet and Society*: *https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity*

Centre for Internet and Society. (2021, July 22). Centre for Internet and Society YouTube. Retrieved from *Nigeria's Digital ID: The Blueprint*: *https://www.youtube.com/watch?v=nlSfw2XW1s8*

Hersey, F. (2020, August 5). Verify my life: could a Nigerian problem lead to a global trust solution? Retrieved from *Biometric Update*: *https://www.biometricupdate.com/202008/verify-my-life-could-a-nigerian-problem-lead-to-a-global-trust-solution*

Human Rights Watch. (2021). World Report 2021. Retrieved from *Human Rights Watch*: *https://www.hrw.org/world-report/2021/country-chapters/nigeria*

ID4Africa. (2020, September 23). YouTube. Retrieved from *Nigeria's Identity Ecosystem*. [video]: *https://www.youtube.com/watch?v=OgcKzQ8I7_U&t=4425s*

Macdonald, A. (2021, March 2). Biometric Update. Retrieved from Nigerian State makes digital ID numbers mandatory to access government services: *https://www.biometricupdate.com/202103/nigerian-state-makes-digital-id-numbers-mandatory-to-access-government-services*

Macdonald, A. (2021, May 13). Nigeria reiterates crucial role of biometric national ID, updates SIM registration policy. Retrieved from *Biometric Update*: *https://www.biometricupdate.com/202105/nigeria-reiterates-crucial-role-of-biometric-national-id-*

updates-sim-registration-policy

Macdonald, A. (2021, February 2). Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit. Retrieved from *Biometric Update*: *https://www.biometricupdate.com/202102/nigerias-move-to-link-digital-identity-numbers-to-sim-cards-sparks-lawsuit*

National Identity Management Commission. (2007, December). Advertisement Privacy Impact Assessment Study. Retrieved from *National Identity Management Commission*: *https://www.nimc.gov.ng/docs/adverts/RFP_for_Project_PIA.pdf*

National Identity Management Commission. (2007). National Identity Management Commission Act 2007. Retrieved from *National Identity Management Commission*: *https://www.nimc.gov.ng/docs/reports/nimc_act.pdf*

National Identity Management Commission. (2015, August 31). Mandatory Use of NIN Now January 2016, Plans Smart Enrolment. Retrieved from *NIMC*: *https://nimc.gov.ng/mandatory-use-of-nin-now-january-2016-plans-smart-enrolment/*

National Identity Management Commission. (2017). Access to Registered Information in the National Identity Database Regulations. Retrieved from *National Identity Management Commission*: *https://nimc.gov.ng/docs/NIMCaccess_register.pdf*

National Identity Management Commission. (2017). Privacy and Security Policy. Retrieved from *National Identity Management Commission*: *https://nimc.gov.ng/docs/pia_policy.pdf*

National Identity Management Commission. (2017). Privacy Impact Assessment Report. Retrieved from *National Identity Management Commission*: *https://nimc.gov.ng/docs/pia_report.pdf*

National Identity Management Commission. (2021). Retrieved from *National Identity Management Commission*: *https://nimc.gov.ng/*

National Identity Management Commission. (2021). Enrolment Dashboard June 2021. Retrieved from *NIMC*: *https://nimc.gov.ng/enrolment-dashboard-june-2021/*

National Identity Management Commission. (2021). Enrolment Page. Retrieved from *National Identity Management Commission*: *https://nimc.gov.ng/enrolment-form/*

National Identity Management Commission. (2021). How to Enrol (Adults). Retrieved from *NIMC*: *https://nimc.gov.ng/how-to-enrol-adults/*

National Identity Management Commission. (2021). NIMC mobile app. Retrieved from *National Identity Management Commission*: *https://nimcmobile.app/*

National Identity Management Commission. (2001). Sagem S.A. France - Closure of 2001 Agreement and Handover of the Nigerian National Identity Card

Project - The issues. Retrieved from *NIMC*: *https://www.nimc.gov.ng/docs/sagem%20handover%20issues.pdf*

National Information Technology Development Agency. (2019). Nigeria Data Protection Regulation. Retrieved from *National Information Technology Development Agency*: *https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf*

Nigerian Communications Commission. (2020). Data Protection Bill . Retrieved from *Nigerian Communications Commission*: *https://www.ncc.gov.ng/docman-main/legal-regulatory/legal-other/911-data-protection-bill-draft-2020/file*

Nigerian Communications Commission. (2021, July 25). PRESS STATEMENT: FG Extends NIN-SIM Verification Deadline to October 31 2021. Retrieved from *NCC*: *https://www.ncc.gov.ng/media-centre/news-headlines/1032-press-statement-fg-extends-nin-sim-verification-deadline-to-october-31-2021#*

Nigerian Communications Commission. (2021, May). Revised National Identity Policy for SIM Card Registration. Retrieved from Nigerian Communications Commission: *https://www.ncc.gov.ng/docman-main/legal-regulatory/legal-other/988-revised-national-identity-policy-for-sim-card-registration/file*

Office of the National Security Adviser. (2021, February 24). National Cybersecurity Policy and Strategy. Retrieved from Office of the National Security Adviser Counter Terrorism Centre: *http://ctc.gov.ng/wp-content/uploads/2021/02/NATIONAL-CYBERSECURITY-POLICY-AND-STRATEGY-2021_E-COPY_24223825.pdf*

Ohia, P. (2012, September 6). Nigeria: French Firm Fined 500,000 Euros for Bribing Nigerian Officials. Retrieved from *All Africa*: *https://allafrica.com/stories/201209060099.html*

Okere, A. (2019, August 31). NIMC needs N132bn to register 200 million Nigerians – Aziz, DG. Retrieved from *The Punch*: *https://punchng.com/nimc-needs-n132bn-to-register-200-million-nigerians-aziz-dg/*

Okonji, E. (2019, August 8). ThisDay. Retrieved from ICT Stakeholders Urge Buhari to Sign Data Protection Bill: *https://www.thisdaylive.com/index.php/2019/08/08/ict-stakeholders-urge-buhari-to-sign-data-protection-bill/*

Premium Times. (2016, February 28). Nigeria announces removal of 23,846 ghost workers from government payroll. Retrieved from *Premium Times*: *https://www.premiumtimesng.com/news/top-news/199246-nigeria-announces-removal-of-23846-ghost-workers-from-government-payroll.html*

Proshare. (2020, February 5). REGULATORY CONVERSATIONS 6.0: NIN: Matters Arising and Implications To Nation Building. Retrieved from *Proshare*: *https://bit.ly/3i5DOUy*

Slater, J. (2018, July 10). India is no longer home to the largest number of poor people in the world. Nigeria is. Retrieved from *The Washington Post*: *https://www.washingtonpost.com/news/worldviews/wp/2018/07/10/india-is-no-longer-home-to-the-largest-number-of-poor-people-in-the-world-nigeria-is/*

UNICEF. (2019, December 11). Despite significant increase in birth registration, 17 Million of Nigeria's children remain 'invisible' – UNICEF. Retrieved from *UNICEF*: *https://www.unicef.org/nigeria/press-releases/despite-significant-increase-birth-registration-17-million-nigerias-children-remain*

Vanguard. (2018, September 20). Mandatory use of national ID numbers begins January 2019. Retrieved from *Vanguard*: *https://www.vanguardngr.com/2018/09/mandatory-use-of-national-id-numbers-begins-january-2019/*

VerifyMe. (2021, July). About us. Retrieved from VerifyMe: *https://verifyme.ng/about*

World Bank. (2016). Identification for Development (ID4D) Country Diagnostic: Nigeria. The World Bank.

World Bank. (2020, February 18). Nigeria - Digital Identification for Development Project. Retrieved from The World Bank: *https://www.worldbank.org/en/news/loans-credits/2020/02/18/nigeria-digital-identification-for-development-project*

World Bank. (2021). ID4D: Identification for Development. Retrieved from Practitioner's Guide: *https://id4d.worldbank.org/guide/types-id-systems*

World Bank. (2021, July). Practitioner's Guide: Creating a good ID system presents risks and challenges, but there are common success factors. Retrieved from The World Bank: *https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors*

World Bank. (2021). The World Bank Data. Retrieved from Population, total - Nigeria: *https://data.worldbank.org/indicator/SP.POP.TOTL?locations=NG*

World Bank. (2021). The World Bank Data. Retrieved from GDP (Current $US): *https://data.worldbank.org/indicator/NY.GDP.MKTP.CD*

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. ■