Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Digital identity for development should keep pace with national cybersecurity capacity: Nigeria in focus

Babatunde Okunoye

To cite this article: Babatunde Okunoye (2022) Digital identity for development should keep pace with national cybersecurity capacity: Nigeria in focus, Journal of Cyber Policy, 7:1, 24-37, DOI: 10.1080/23738871.2022.2057865

To link to this article: https://doi.org/10.1080/23738871.2022.2057865

Published online: 01 Apr 2022.

JOURNAL OF CYBER POLICY
2022, VOL. 7, NO. 1, 24–37
https://doi.org/10.1080/23738871.2022.2057865

Digital identity for development should keep pace with national cybersecurity capacity: Nigeria in focus

Babatunde Okunoye

Berkman Klein Centre for Internet and Society, Harvard University, Cambridge, USA; Department of Journalism, Film and Television, University of Johannesburg, Johannesburg, South Africa

ABSTRACT

Target 16.9 of the United Nations (UN) Sustainable Development Goals (SDGs) is the provision of legal identity for all, including birth registration by 2030. Approximately 1 billion people globally do not have basic ID credentials. To close this gap, governments in developing countries, including Nigeria, with the backing of international agencies like the World Bank, have launched digital identity schemes for residents. These schemes typically include smart cards which are required to access public and private services. The speed of implementation of these projects has come at the expense of a thorough consideration of cybersecurity and privacy. This is set against the backdrop of the rising threat of cybersecurity breaches in the world against targets such as national identity databases. This paper seeks to provide an overview of digital identity in Nigeria and use the Oxford Global Cyber Security Capacity Centre's Cybersecurity Maturity Model Report 2019 for Nigeria to illustrate how, although progress has been made in key sectors, the implementation of the Nigeria's digital identity programme has progressed faster than cybersecurity maturity in the country. This increases the risk of cyberattacks and opens both the national identity database and users of the digital identity to security vulnerabilities.

ARTICLE HISTORY
Received 12 July 2021
Revised 8 January 2022
Accepted 8 February 2022

KEYWORDS
Digital identity; cybersecurity and privacy; Nigeria; UN SDGs

Introduction

Target 16.9 of the UN Sustainable Development Goals is the provision of legal identity for all, including birth registration by 2030 (United Nations 2021). Nevertheless, approximately 1 billion people globally do not have basic ID credentials. This includes one in four children and young people who do not have birth registration. Another 3.4 billion individuals have IDs but have limitations using them across digital platforms (The World Bank 2019). To close this gap, governments in developing countries, backed by international development agencies such as the World Bank, have launched digital identity schemes to enable identification, verification and authentication services for residents. These schemes typically include smart cards which are required to access public services and complete transactions in the global digital economy.

CONTACT Babatunde Okunoye ✉ bokunoye@cyber.harvard.edu

In some country contexts, the speed of implementation of these projects has come at the expense of a thorough consideration of cybersecurity and privacy. This is set against the backdrop of the rising incidence of cybersecurity breaches in the world. Breaches of public and private enterprises have continued unabated in developed and developing countries. Identity databases are vulnerable to cyberattacks and accidental breaches, as exemplified by the breach, in 2015, of the Office of Personnel Management (OPM), the human resources arm of the United States federal government (Koerner 2016). Data for at least 21 million government employees, contractors and their relations was breached by hackers. Also in the United States in 2015, the data of 191 million voters was leaked on the internet because of a wrongly configured database (Finkle and Volz 2015). This breach exposed sensitive personal information (for example names, addresses, emails, dates of birth and party affiliations) of voters across the country. Furthermore, in the United States in 2009, a data breach occurred in the National Archives and Records Administration (NARA) when a hard drive was sent to an IT contractor for repairs. It stored sensitive information for 76 million veterans (Lord 2020). Most recently, in September 2021, Argentina's National Identity Register (Renaper) was breached by hackers who accessed the personal information of millions of people (scans of ID cards, full names, photographs, home addresses, ID card issuance and expiry dates, social security numbers, citizen numbers, and labour identification codes) and put it on sale on the dark web (Cimpanu 2021). Large data breaches of these types leave populations vulnerable to identity theft or phishing attacks, possibly leading to financial losses.

Nigeria itself is no stranger to cyberattacks. The EndSARS protests of October 2020, where Nigerian youths protested against police brutality (Chutel 2021), showed clearly that government digital assets become vulnerable in conflicts. During the protests, the websites and social media handles of important government departments such as the police, central bank, Economic and Financial Crimes Commission, Independent National Electoral Commission and National Broadcasting Commission were hacked (Sanni 2020), compromising data and disrupting the business of government. As Nigeria's digital identity database becomes more developed and integrated into public and private transactions, as envisaged by section 17 of the National Identity Management Commission Act (National Identity Management Commission 2007), its value will increase, making it a worthwhile target for cyber exploits. The possibility of a data breach of the identity database in the future is not far-fetched. This paper links some of the technical flaws in the implementation of Nigeria's digital identity programme to already identified weaknesses in Nigeria's cybersecurity capacity maturity (Global Cyber Security Capacity Centre 2019) and also draws evidence from expert interviews with cybersecurity professionals in Nigeria.

This paper contributes to the literature on the role of digital identity in development. On this there is no consensus – while it is acknowledged that digital identity programmes help nations achieve developmental outcomes (Martin and Taylor 2021; Masiero and Bailur 2021) such as maintaining security, enabling government social transfers, eliminating fraud in government payrolls, and facilitating effective national planning, some experts aver that these goals might still be achieved with conventional (non-digital) identity systems (AccessNow 2018) and argue that digitising identity enables the powers of digitally-linked government surveillance (Bennett and Lyon 2021) which might lead to human rights abuses. Hence there is a conflict between the role of digital identity as a force for good or for harm (Weitzberg et al. 2021). While there are merits on both sides of the intellectual debate, cybersecurity breaches of large, centralised national digital identity databases like that of Argentina in 2021 (Cimpanu 2021) only strengthen the argument for digital identity potentially causing harm.

An overview of Nigeria's digital identity system

Nigeria has had three digital identity systems. In 1978, the Federal Ministry of Interior, through its agency, the Department of National Civic Registration (DNCR), enrolled Nigerians who were 18 years or older and issued national identity cards after collecting biographical data. The aims of this inaugural project were to use the identity programme as an effective policy mechanism for controlling illegal immigration, to validate other civic documents like international travel passports, and to implement a trusted personal identification system for protecting commercial transactions with financial institutions (Osunade, Olanrewaju, and Phillips 2013). This programme failed after 18 months for reasons yet unclear. The second attempt, in 2001, was also initiated by the DNCR but was private sector-led, costing the government $236.8 million to complete the registration of 52.6 million people, out of a planned 60 million. However, identity cards were only issued to 37.3 million people. This second project was also abandoned in 2006 following corruption investigations relating to the award of the contract (World Bank 2016).

Nigeria's ongoing attempt at digital identification is its third. It commenced in 2007 with the passage of the National Identity Management Commission (NIMC) Bill (National Identity Management Commission 2007) by the Nigerian lawmakers between 17 and 23 May 2007 in the country's bicameral legislature. The Bill was signed by the president of Nigeria on 25 May 2007. The resulting NIMC Act also established the National Identity Management Commission (NIMC) (which replaced the DNCR), an agency under Nigeria's Ministry of Communications and Digital Economy.

The central feature of Nigeria's digital identity scheme is the National Identity Number (NIN). The NIN is an 11-digit number at the heart of the digital identity and is conferred upon the recording of enrolment data of citizens and legal residents, including personal information (for example name, date of birth and place of origin), physical features (for example gender, height and hair colour), residence status (for example address, nationality, country of residence, etc.), personal reference numbers (for example driver's licence, passport number and National Insurance number) and biometric data (photograph and fingerprints). The enrolment form is accessible on the website of NIMC (NIMC 2021). This enrolment data is captured by NIMC through over 1060 NIMC-operated registration centres. Mobile network operators and partner agencies, such as the National Population Commission, Independent National Electoral Commission and Nigerian Immigration Service have also been drafted in as registration centres in a bid to get to a total of at least 9,000 registration centres estimated to be sufficient to cover Nigeria's population of over 200 million people (ID4Africa 2020). After enrolment, data is stored in a centralised database administered by the NIMC and is used for verification and authentication of identity in transactions with a host of organisations in the public and private sectors. The NIN registration attained a coverage of over 70 million as at November 2021, with the country's commercial capital, Lagos State, having the highest enrolment number of over 8 million (National Identity Management Commission 2021). A stated goal of the digital identity programme is to issue a national identity (smart) card alongside the NIN. Nigeria's digital identity also includes a mobile app for authentication and verification purposes (National Identity Management Commission 2021).

The policy objectives of Nigeria's digital identity project are similar to many others around the world and include cutting the prohibitive costs of having duplicate identity cards; tackling insecurity by enabling proper identification of the residents of a country; facilitating government social transfers; eliminating fraud in government payroll management; and empowering millions who had been excluded from public and private transactions such as accessing banking services and voting due to a lack of identity documents (World Bank 2020).

Section 27 of the NIMC Act, entitled 'Mandatory use of National Identification Number (NIN)', envisages that the NIN will be presented for transactions such as the opening of bank accounts, SIM card registration, the purchase of insurance policies, payment of taxes and voter registration (Okunoye 2021). The process towards realising this began in January 2019, when the government announced that having a NIN was mandatory. The long-term plan is to harmonise the digital identity with other functional identities in operation in the country, such as bank verification number, driver's licence, international passports, and voter's card (ID4D 2020).

Nigeria's cybersecurity capacity maturity

In 2018, the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford reviewed the maturity of cybersecurity capacity in Nigeria at the request of the Office of the National Security Adviser (ONSA), the government office responsible for cybersecurity in Nigeria (Global Cyber Security Capacity Centre 2019). The GCSCC is an international research centre based at Oxford University's Department of Computer Science, which focuses on cybersecurity capacity-building across the world. The GCSCC created the Cybersecurity Maturity Model (CMM) model (Global Cyber Security Capacity Centre 2021) to review cybersecurity capacity for nations to help them 'to self-assess, benchmark, better plan investments and national cybersecurity strategies, as well as set priorities for capacity development' (Global Cyber Security Capacity Centre 2021). The CMM assesses the maturity of nations across five dimensions of cybersecurity capacity, namely Cybersecurity Policy and Strategy, Cyber Culture and Society, Cybersecurity Education, Training and Skills, Legal and Regulatory Frameworks, and Standards, Organizations and Technologies. The CMM has been deployed more than 120 times in over 87 nations (Table 1).

Each CMM dimension has factors which describe what it means for nations to possess cybersecurity capacity: each factor, in turn, consist of aspects, and for each aspect there are indicators, which describe steps and actions that, once observed, define the state of maturity of that aspect (Global Cyber Security Capacity Centre 2021). The CMM describes five stages of maturity, quoted below from the Global Cyber Security and Capacity Centre, ranging from the start-up stage to the dynamic stage (Global Cyber Security Capacity Centre 2021):

(1) Start-up: 'At this Stage, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but

Table 1. CMM dimensions and factors which measure national cybersecurity capacity and maturity.

	Dimensions				
	Cybersecurity Policy and Strategy	Cyber Culture and Society	Cybersecurity Education, Training and Skills	Legal and Regulatory Frameworks	Standards, Organizations and Technologies
Factors	National cybersecurity strategy	Cybersecurity mind-set	Awareness-raising	Formal and informal cooperation frameworks to combat cybercrime	Adherence to standards
	Incident response	Trust and confidence on the internet	Framework for education	Criminal justice system	Internet infrastructure resilience
	Critical infrastructure protection	User understanding of personal information protection online	Framework for professional training	Legal frameworks	Software quality
	Crisis management	Reporting mechanisms			Technical security controls
	Cyber defence consideration	Media and social media			Cryptographic controls
	Communications redundancy				Cybersecurity marketplace
					Responsible disclosure

no concrete actions have been taken. There may be an absence of observable evidence at this Stage'.

(2) Formative: 'Some features of the Aspect have begun to grow and be formulated, but may be ad hoc, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated'.

(3) Established: 'The Indicators of the Aspect are in place, and evidence shows that they are working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the Aspect. But the Aspect is functional and defined'.

(4) Strategic: 'Choices have been made about which parts of the Aspect are important, and which are less important for the particular organisation or nation. The strategic Stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances'.

(5) Dynamic: 'At this Stage, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this Stage'.

The GCSCC's assignment of maturity stages is based upon their research methodology (Global Cyber Security Capacity Centre 2021; Creese, Dutton, and Esteve-Gonzalez 2021) reflected through evidence collected, including reports by stakeholders, desktop research and the professional judgement of research staff.

Nigeria's CMM report indicated a maturity stage above formative for only three factors – 'Trust and Confidence on the Internet', 'Framework for Education', and 'Formal and Informal Cooperation Frameworks to combat Cybercrime' across five dimensions. All other 21 factors across five dimensions of maturity were adjudged either at start-up or formative stage. This suggests opportunities for investment in maturity of these identified areas in Nigeria, perhaps especially across the factors adjudged start-up or formative – precisely the purpose of the maturity assessment, which goes on to make a comprehensive list of recommendations for strengthening the identified areas. Although this paper delves further into policy recommendations in its conclusion, there is a link between Nigeria's identified strengths and weaknesses in its maturity review and some of the technical implementations identified in this paper, which might present immediate areas of investment:

(1) When the USSD flaw described below was identified by civil society in Nigeria and reported to NIMC, according to a cybersecurity expert interviewed for this research, it took three months for it to be rectified. Although closer to a privacy issue than a strict cybersecurity issue, the long response time might further highlight the need for the strengthening of incidence response, a factor under the dimension 'Cybersecurity Policy and Strategy', already identified for strengthening with important recommendations in Nigeria's CMM report.

(2) From interviews with cybersecurity experts in Nigeria, the challenges with the NIMC app below, before a stable version was released, might point to lapses in technical development processes which do not sufficiently take inputs from cybersecurity experts outside of close public circles. This might be a recurring trend, as seen with challenges with the launch of Nigeria's e-Naira app (Benson 2021; Ladipo and Udugba 2021) and might point to the need for strengthening the factor 'Adherence to Standards' under the dimension 'Standards, Organizations and Technologies' already identified for strengthening with useful recommendations in Nigeria's CMM report.

(3) Data from interviews with cybersecurity experts in Nigeria also suggest that a bane of individuals' incidence reporting in Nigeria might be the fraught relationship Nigerians have had with law enforcement, where people reporting incidents in the past were viewed with suspicion. This might point to the urgent need to strengthen the factor 'Criminal Justice System' under the Dimension 'Legal and Regulatory Frameworks' for which Nigeria's CMM report also provides useful recommendations for improvement.

Gaps in the implementation of Nigeria's digital identity system

The implementation of Nigeria's national ID programme divulged gaps which relate to aspects of the CMM report for Nigeria, highlighting urgent areas where cybersecurity capacity needs strengthening.

USSD for accessing national identity numbers

One of the earliest flaws in the implementation of Nigeria's digital identity scheme was a USSD code on mobile phones which permitted anyone with the date of birth and

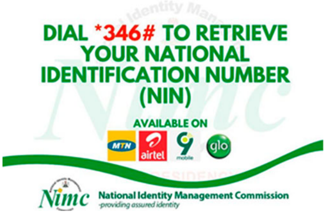

Figure 1. A message from the National Identity Management Commission on USSD codes for accessing National Identity Numbers (NIN).

surname of any Nigerian to access their NIN (Paradigm Initiative 2019). This implementation, although well-intentioned, to allow easy access to NIN data by millions of Nigerians, inadvertently led to a serious privacy breach. The information required to access the NIN of Nigerians was for many people easily obtainable, sometimes even publicly available. This flaw was identified by a coalition of civil society organisations in Nigeria, including Paradigm Initiative (Figure 1).

The NIN was designed as a unique identifier for Nigerian citizens and residents and was planned to be linked with all other functional identities in the country. Inadvertently enabling access to the NIN via easily accessible information exposed millions of Nigerians to possible identity theft and, more probably, in the context of Nigeria and the stage of integration of the NIN with other national records, social engineering attacks such as phishing.

Although the breach itself was worrisome, more worrisome was the slow response of NIMC to address it. When this flaw was first identified shortly after the announcement of Nigeria's digital identity ecosystem in September 2018 (Adegoke 2020), the USSD code flaw was only rectified after litigation brought by civil society in Nigeria in January 2019 and judgment by a federal high court in Nigeria in June 2019 (Andersen 2019). One of the mechanisms used to correct the flaw was that the NIN could now only be accessed via the phone number used in NIN registration, and not just any mobile number (National Identity Management Commission 2021).

Privacy concerns have persistently dogged Nigeria's digital identity project. In December 2021, the government released an updated ID policy (Nigerian Communications Commission 2020) which mandated the linking of the NIN with SIM cards of Nigerian residents. Given the government's history of covert surveillance of citizens (Ilori 2021), this development was met with stiff resistance from sections of the public who feared it was another toolkit for government surveillance. This perceived privacy intrusion was made more urgent by the absence of a data protection law in Nigeria. The process for drafting a data protection bill seemed threatened in November 2021 with the publicly advertised call for consultants to collaborate with the National Identity Management Commission (NIMC) to create a new document (Omoniyi 2021) while the current draft (Nigerian Communications Commission 2020) is still awaiting passage into law. The Nigerian Data Protection Regulation (NDPR) (NITDA 2019) enacted by the National Information Technology Development Agency (NITDA) is the major policy document regulating privacy in the country, alongside sector-specific legislation such as that covering financial services, telecommunications, and children's rights which provide limited privacy protections. The Cybercrime Act

(Computer Emergency and Response Team 2015) is also a major policy document governing cybercrime.

National identity app malfunction

Another implementation gap in Nigeria's digital identity scheme which exposed citizens' data is the digital identity mobile app. The mobile app was designed to be downloaded from app stores (Apple and Google) and installed on smartphones as a means of verification and authentication of holders of the digital identity (National Identity Management Commission 2021). The mobile app provides verification as a service to its users, which it categorised as pay-as-you go, individual and corporate. The most current version as at the time of this research is dated 3 June 2021. Users can download the digital app from the phones used to register for their national identity.

Earlier versions of the digital identity app displayed implementation flaws such that, when users downloaded the app from smartphone app stores using the phone numbers they had used in registering for the digital identity, the digital identities downloaded were those of other Nigerians – thereby displaying the credentials of strangers (Kolawole 2020). An example of this problem was highlighted on Twitter (Ifeoma 2020). NIMC were quick to respond to the public outrage which met this implementation (National Identity Management Commission 2020) and have since released several updates of the app which solved the problem. The most recent version of the app can be accessed on NIMC's website (National Identity Management Commission 2021).

Phishing websites and apps designed to harvest national identity data

Another cybersecurity gap in the implementation of Nigeria's digital identity project, attested to by cybsersecurity experts in the country, was the insufficient public awareness regarding potential cybersecurity risks associated with digital identity. Cybersecurity breaches have been on the increase in Nigeria (Deloitte 2021) in a country context where, according to the GCSCC maturity estimates, most of the factors under the cybersecurity dimensions 'Cyber Culture and Society' and 'Cybersecurity Education, Training and Skills' are at the start-up or formative stage. The relevance of both of these maturity dimensions to cybersecurity is that they relate to the capacity of the broader public to understand and mitigate cybersecurity risks. In the CMM report for Nigeria (Global Cyber Security Capacity Centre 2019), the dimension 'Cybersecurity Education, Training and Skills' has as one of its factors 'Awareness Raising' on cybersecurity, which was evaluated as being 'formative'. Nigeria's CMM report describes 'Awareness Raising' in Nigeria as 'formative', stating that 'although pockets of awareness-raising activity exist, there is no over-arching continuous effort on a national level'. This potentially affects the cybersecurity of Nigeria's digital identity system – if awareness-raising around the cybersecurity risks to which users of the ID are vulnerable is inadequate, this makes many users more vulnerable to a cybersecurity breach. The CMM report proceeds to provide recommendations to improve awareness-raising. The importance of a nationally-directed cybersecurity awareness campaign can be seen from the example of the United Kingdom where governmental organisations are actively involved in messaging and awareness-raising on the threats posed by cybercriminals seeking to prey on people (South East Regional Organized Crime

Unit 2021; Metropolitan Police 2021). This public messaging is even more important for vulnerable groups like the elderly (Age UK 2021) who may not be as technologically savvy as younger citizens.

The digital ID-linked cybersecurity threat citizens face is real. In December 2020, the Nigerian Ministry of Communications and Digital Economy announced the directive that all Nigerians link their National Identity Numbers with their SIM cards (Nigerian Communications Commission 2020) and created channels online and via the USSD services of the mobile phone networks in the country to do so. A stated purpose of this directive was to 'improve the integrity and transparency of the SIM registration process' (Nigerian Communications Commission 2020). The mandatory SIM registration was implemented to stop criminals from using unregistered SIMs (George 2020). Following this directive, websites and applications (Olatunji 2021) appeared online offering to help Nigerians link their NIN to their SIMS. These websites usually requested that users fill out a form requiring sensitive personal information. They were actually attempts by cybercriminals to harvest the personal information of Nigerians for use in phishing and identity theft schemes, as alluded to in a timely press statement by NIMC (Olatunji 2021).

The response of NIMC in releasing a press statement on their website and on social media was quick and commendable. Nevertheless, a more extensive public awareness-raising preceding the national roll out of a digital identity scheme would have been a more appropriate effort to protect users of the digital identity.

Conclusion and recommendations

Cybersecurity breaches have dominated news headlines in the year 2021. The most recent at the time of writing are the breach of Argentina's national identity database in September 2021 (Cimpanu 2021) and the global ransomware attack centred on the US information technology firm Kaseya, affecting at least 1500 organisations around the world, with the attackers making a demand of $70 million as ransom (Satter 2021). The rising spate of cyberattacks across the world, and the many breaches of government databases in the past (some mentioned in this paper) should refocus the attention of NIMC on best cybersecurity practices because no country or region is immune to this threat. Some of the digital security gaps highlighted in this paper, and a review of Nigeria's digital identity project, suggest more attention can be given to the real cybersecurity threats to which a large national identity database is exposed.

Many cybersecurity breaches in history, including some of those of government databases mentioned in this paper can be traced to human error – such as a misconfigured database, as with the breach of US voters' data (Finkle and Volz 2015), hard drives not wiped clean before transfer, as with the breach at the National Archives and Records Administration (Lord 2020), and a successful phishing email targeted at staff, such as with the case of the breach at the Sony Corporation in 2014 (Keizer 2015). The breach of Argentina's national identity database was also linked with human error of government staff (Cimpanu 2021) who had access to the identity database. And although not explicitly elucidated in this paper, another critical gap in digital identity systems design is the centralisation of databases (such as in Nigeria) which makes data vulnerable because it presents a single point of failure (AccessNow 2018) for hackers, as seen with the Argentina breach where data was centralised. A relevant policy recommendation for the design of digital identity systems might then be that, at a minimum, digital identity databases should be decentralised, for instance by storing data in regions of collection, rather than collating and storing all identity data in a centralised database.

It is important to note, however, that in the context of Nigeria's public institutions' cybersecurity readiness, NIMC has made important strides as is considered a leader. The CMM report for Nigeria (Global Cyber Security Capacity Centre 2019) commends NIMC as an example of a government agency where cybersecurity best practice is being followed, with structured cybersecurity polices and controls. However, a successful breach of the NIMC database which publicly exposes citizens' data could be a major event and could dampen public confidence in the laudable digital identity project, thus derailing it. The CMM report for Nigeria suggests a plan of action to improve cybersecurity capacity through its recommendations. The gaps identified in this paper relate largely to the cybersecurity capacity dimensions 'Cyber Culture and Society' and 'Cybersecurity Education, Training and Skills'. It is important that the recommendations under those dimensions at the end of the CMM review are implemented thoroughly. Particularly urgent for NIMC is the need for the training and retraining of staff and contractors who interface with the national identity database. It is commendable that Nigeria's Cybersecurity Policy and Strategy 2021 (Office of the National Security Adviser 2021) also makes many of these recommendations, and it is hoped that they will be implemented at the sectoral level, including at NIMC.

An ongoing research interest of the author, which might further this work, is to understand the nature of public and private sector collaboration for cybersecurity in Nigeria. Nigeria's revised cybersecurity policy lists several government agencies as responsible for cybersecurity while recognising the role of civil society and the private sector in securing the nation's cyberspace. Little research has been done to understand how (or if) these agencies collaborate in the face of the nation's push for a digital economy exemplified by the renaming of the Ministry of Communications to the Ministry of Communications and Digital Economy in October 2019 (Kazeem 2019) in line with the nation's Economic Growth and Recovery Plan (State House 2020) and the launch of the nation's electronic wallet – the e-naira – in October 2021 (Ree 2021). Nigeria's cybersecurity policy acknowledges that the increasing digitisation of the economy comes with its attendant cybersecurity risks.

Acknowledgments

The author wishes to thank his previous employer, Paradigm Initiative, Lagos Nigeria for the introduction to aspects of research into digital identity in Nigeria. Profound gratitude is owed to Research ICT Africa Cape Town South Africa, for collaboration on a project assessing the state of digital identity in Africa and Nigeria (Research ICT Africa 2021; Okunoye 2021) which got him thinking more deeply about the socio-legal and socio-technical aspects of digital identity for development. The author also wishes to thank the expert interviewees who provided insight on Nigeria, two anonymous reviewers and the Journal's editors for their very detailed feedback which greatly improved the original manuscript.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Babatunde Okunoye is a Fellow with the Berkman Klein Centre for Internet and Society, Harvard University, where his research focuses on Information and Communication Technologies for Development (ICT4D), particularly how public and commercial datasets can spur development in the Global South. He is also a research student at the Department of Journalism, Film and Television at the University of Johannesburg South Africa where he is researching the lived experiences of marginalized urban communities (slum dwellers) in Nigeria with the national (digital) identity.

References

AccessNow. 2018. National Digital Identity Programmes: What Next? AccessNow. Accessed 6 July 2021. https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf.

Adegoke, Adeboye. 2020. *Digital Rights and Privacy in Nigeria*. Abuja: Paradigm Initiative. Accessed 4 July 2021. https://ng.boell.org/sites/default/files/2020-08/Digital%20Rights%20and%20Privacy%20in%20Nigeria_0.pdf.

Age UK. 2021. "Staying Safe Online." *Age UK*. Accessed 7 July 2021. https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/#skipToContent.

Andersen. 2019. "Federal High Court Affirms the Data Privacy Rights of Nigerian Citizens." *Andersen*, August 30. Accessed 6 July 2021. https://ng.andersen.com/federal-high-court-affirms-the-data-privacy-rights-of-nigerian-citizens/.

Bennett, Colin, and David Lyon. 2021. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. New York: Routledge.

Benson, Emmanuel A. 2021. "3 days after launch, it's been a rough patch for the eNaira; here's what you need to know." *Business Insider Africa*, October 28. Accessed 6 January 2022. https://africa.businessinsider.com/local/markets/3-days-after-launch-its-been-a-rough-patch-for-the-enaira/3d1ckgj.

Chutel, Lynsey. 2021. "Nigerian Security Forces Shot Protesters. Will They Ever Face Justice?" *Foreign Policy*, February 3. Accessed 4 July 2021. https://foreignpolicy.com/2021/02/03/nigeria-police-security-forces-endsars-protests-lagos-investigation-justice-accountability/.

Cimpanu, Catalin. 2021. "Hacker steals government ID database for Argentina's entire population." *The Record*, October 18. Accessed 1 January 2022. https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/.

Computer Emergency and Response Team. 2015. "Cybercrime Act 2015." *Computer Emergency and Response Team*. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf.

Creese, S., W. H. Dutton, and P. Esteve-Gonzalez. 2021. "The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions." *Personal and Ubiquitous Computing* 25 (5): 941–955.

Deloitte. 2021. "A Fresh Perspective: Nigeria Cyber Security Outlook 2021." *Deloitte*. Accessed 7 July 7 2021. https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2021.html#.

Finkle, Jim, and Dustin Volz. 2015. "Database of 191 million U.S. voters exposed on Internet: researcher." *Reuters*, December 29. Accessed 4 July 2021. https://www.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229?edition-redirect = uk.

George, Libby. 2020. "Nigeria gives Telecom providers two weeks to add ID numbers to SIM cards – statement." Nasdaq, December 15. Accessed 7 July 7 2021. https://www.nasdaq.com/articles/nigeria-gives-telecoms-providers-two-weeks-to-add-id-numbers-to-sim-cards-statement-2020.

Global Cyber Security Capacity Centre. 2019. *Cybersecurity Capacity Review: Nigeria. Available upon Request from the Global Cyber Security Capacity Centre*. Oxford: Global Cyber Security Capacity Centre.

Global Cyber Security Capacity Centre. 2021. "Cybersecurity Capacity Maturity Model for Nations (CMM). 2021 Edition." *Global Cyber Security Capacity Centre*, March. Accessed 4 January 2022. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

Global Cyber Security Capacity Centre. 2021. "Global Cyber Security Capacity Centre." *University of Oxford*. Accessed 6 July 2021. https://gcscc.ox.ac.uk/.

Global Cyber Security Capacity Centre. 2021. "Global Cyber Security Capacity Centre." University of Oxford. Accessed 6 July 2021. https://gcscc.ox.ac.uk/cmm-reviews#/.

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

ID4D. 2020. "Nigeria's Identity Ecosystem." *YouTube*, September 23. Accessed 5 July 2021. https://www.youtube.com/watch?v = OgcKzQ8I7_U&t = 4425s.

Ifeoma. 2020. "@i_feoma." *Twitter*, August 15. Accessed 6 July 2021. https://twitter.com/i_feoma/status/1294656862944669696.

Ilori, Tomiwa. 2021. *Status of Surveillance in Nigeria: Refocusing the Search Beams*. Abuja: Paradigm Initiative. Accessed 1 February 2021. https://paradigmhq.org/wp-content/uploads/2021/04/Policy-Brief-009-Status-of-Surveillance-in-Nigeria.pdf.

Kazeem, Yomi. 2019. "Nigeria's tech leaders aren't convinced by a government plan to reframe its focus on their sector." *Quartz Africa*, October 24. https://qz.com/africa/1734888/nigeria-renames-communications-ministry-to-oversee-tech-industry/.

Keizer, Gregg. 2015. "Sony hackers targeted employees with fake Apple ID emails." *Computer World*, April 23. Accessed 8 July 2021. https://www.computerworld.com/article/2913805/sony-hackers-targeted-employees-with-fake-apple-id-emails.html.

Koerner, Brendan I. 2016. "Inside the Cyberattack That Shocked the US Government." *Wired*, October 23. Accessed 4 July 2021. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Kolawole, Oluwanifemi. 2020. "UPDATED: Why you should not use the NIMC app yet." *Techpoint.africa*, August 17. Accessed 6 July 2021. https://techpoint.africa/2020/08/17/nimc-app-possible-mass-phishing/.

Ladipo, Ebunoluwa, and Tony Udugba. 2021. "CBN updates eNaira wallet app amidst user complaints." *BusinessDay*, October 28. Accessed 6 January 2022. https://businessday.ng/news/article/cbn-updates-enaira-wallet-app-amidst-user-complaints/.

Lord, Nate. 2020. "Data Breaches: Top 10 Biggest Government Data Breaches of All Time in the U.S." *Data Insider*, October 6. Accessed 4 July 2021. https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time.

Martin, Aaron, and Linnet Taylor. 2021. "Exclusion and Inclusion in Identification: Regulation, Displacement and Data Justice." *Information Technology and Development* 27 (1): 50–66.

Masiero, Silvia, and Savita Bailur. 2021. "Digital Identity for Development: The Quest for Justice and a Research Agenda." *Information Technology for Development* 27 (1): 1–12.

Metropolitan Police. 2021. "Cyber crime." *Metropolitan Police*. Accessed 7 July 2021. https://www.met.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/.

National Identity Management Commission. 2007. "National Identity Management Commission (NIMC)." NIMC Act 2007. Accessed 4 July 2021. https://www.nimc.gov.ng/docs/reports/nimc_act.pdf.

National Identity Management Commission. 2020. "@nimc_ng." *Twitter*, 17 August. Accessed 6 July 2021. https://twitter.com/nimc_ng/status/1295465765617926145?s=19.

National Identity Management Commission. 2021. "Enrolment Dashboard November 2021." *NIMC*, November. Accessed 7 January 2022. https://nimc.gov.ng/enrolment-dashboard-november-2021/.

National Identity Management Commission. 2021. "Enrolment Form." *NIMC*. https://nimc.gov.ng/enrolment-form/.

National Identity Management Commission. 2021. "Mobile Digital ID." *NIMC*. Accessed 5 July 2021. https://nimc.gov.ng/mobile-digital-id/.

National Identity Management Commission. 2021. "NIMC Mobile App." *NIMC*. Accessed 6 July 2021. https://nimcmobile.app/.

National Identity Management Commission. 2021. "SMS Services: USSD for NIN Retrieval." *NIMC*. Accessed 6 July 2021. https://nimc.gov.ng/sms-service/.

Nigerian Communications Commission. 2020. "Data Protection Bill 2020." *Nigerian Communications Commission*. Accessed 4 January 2022. https://www.ncc.gov.ng/documents/911-data-protection-bill-draft-2020/file.

Nigerian Communications Commission. 2020. "Press Statement: Implementation of new SIM registration rules." *Nigerian Communications Commission*, 15 December. Accessed 7 July 2021. https://ncc.gov.ng/media-centre/news-headlines/928-press-statement-implementation-of-new-sim-registration-rules.

NITDA. 2019. "Nigeria Data Protection Regulation 2019." *NITDA*. Accessed 4 January 2022. https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf.

Office of the National Security Adviser. 2021. *Office of the National Security Adviser*, February 24. Accessed 10 July 2021. https://ctc.gov.ng/national-cybersecurity-policy-and-strategy/.

Okunoye, Babatunde. 2021. "Digital Identity in Nigeria: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (Towards the Evaluation of Digital ID Ecosystems in Africa: Findings from Ten Countries) [Case study]. Research ICTAfrica." *Research ICT Africa*, November. Accessed 7 January 2022. https://researchictafrica.net/publication/digital-identity-in-nigeria-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/.

Olatunji, Haleem. 2021a. "'Beware of fraudulent app for linking NIN with SIM cards' — NIMC alerts Nigerians." *The Cable*, February 11. Accessed 7 July 2021. https://www.thecable.ng/beware-of-fraudulent-app-for-linking-nin-with-sim-cards-nimc-alerts-nigerians.

Olatunji, Haleem. 2021b. "SCAM ALERT: Website asking for individual NIN registration is fraudulent, says NIMC." *The Cable*, February 11. Accessed 7 July 2021. https://www.thecable.ng/scam-alert-website-asking-for-individual-nin-registration-is-fraudulent-says-nimc.

Omoniyi, Tosin. 2021. "Data Protection: Indignation as FG abandons draft bill, seeks 'consultants' for fresh process." *Premium Times*, November 17. Accessed 4 January 2022. https://www.premiumtimesng.com/news/top-news/495768-data-protection-indignation-as-fg-abandons-draft-bill-seeks-consultants-for-fresh-process.html.

Osunade O., Olanrewaju BS, and Phillips OS. 2013. "A Conceptual Design of a Low Cost Identification Management System for Nigeria." *GESJ: Computer Science and Telecommunications*, 24–32.

Paradigm Initiative. 2019. "National Identity Management Commission – Attorney General of the Federation." *Paradigm Initiative*, August 30. Accessed 6 July 2021. https://paradigmhq.org/wp-content/uploads/2021/04/v.-NATIONAL-IDENTITY-MANAGEMENT-COMMISSION-ATTORNEY-GENERAL-OF-THE-FEDERATION-.pdf.

Ree, Jack. 2021. "Five Observations on Nigeria's Central Bank Digital Currency." *International Monetary Fund News*, November 16. https://www.imf.org/en/News/Articles/2021/11/15/na111621-five-observations-on-nigerias-central-bank-digital-currency.

Research ICT Africa. 2021. "RIA releases 10 country reports on Digital ID framework." *ResearchICTAfrica*, 9 November. Accessed 7 January 2022. https://researchictafrica.net/2021/11/09/ria-releases-10-country-reports-on-digital-id-framework/#_ftn1.

Sanni, Kunle. 2020. "#EndSARS: EFCC admits website was attacked." *Premium Times*, October 19. Accessed 4 July 2021. https://www.premiumtimesng.com/news/top-news/421700-endsars-efcc-admits-website-was-attacked.html.

Satter, Raphael. 2021. "Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says." *Reuters*, July 6. Accessed 8 July 2021. https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/.

South East Regional Organized Crime Unit. 2021. "Phishing Awareness." *ROCU*. Accessed 7 July 2021. https://serocu.police.uk/phishing/.

State House. 2020. "Economic Recovery and Growth Plan." *Statehouse.gov*. Accessed 3 January 2021. https://statehouse.gov.ng/policy/economy/economic-recovery-and-growth-plan/.

United Nations. 2021. "Department of Economic and Social Affairs: Sustainable Development." *United Nations*. Accessed 4 July 2021. https://sdgs.un.org/goals/goal16.

Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. 2021. “Between Surveillance and Recognition: Rethinking Digital Identity in Aid.” *Big Data & Society* 8 (1): 1–7.

World Bank. 2016. *ID4D Country Diagnostic: Nigeria*. Washington DC: The World Bank. Accessed 1 July 2021. https://documents1.worldbank.org/curated/en/136541489666581589/pdf/113567-REPL-Nigeria-ID4D-Diagnostics-Web.pdf.

World Bank. 2019. “Inclusive and Trusted Digital ID Can Unlock Opportunities for the World’s Most Vulnerable.” *The World Bank*, August 14. Accessed 4 July 2021. https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable.

World Bank. 2020. *Project Appraisal Document on a Proposed Credit for the Digital Identification for Development Project*. World Bank. Accessed 4 July 2021. https://documents1.worldbank.org/curated/en/250181582340455479/pdf/Nigeria-Digital-Identification-for-Development-Project.pdf.