Data & Policy (2022), 4: e37
doi:10.1017/dap.2022.29

COMMENTARY

Mistrust of government within authoritarian states hindering user acceptance and adoption of digital IDs in Africa: The Nigerian context

Babatunde Okunoye[1,2,*]

[1]Department of Communication and Media Studies, University of Johannesburg, Johannesburg, South Africa
[2]Berkman Klein Centre for Internet and Society, Harvard University, Cambridge, Massachusetts, USA
*Corresponding author. E-mail: bokunoye@cyber.harvard.edu

Received: 24 November 2021; **Revised:** 27 July 2022; **Accepted:** 27 September 2022

Key words: authoritarianism; digital identity; mistrust; Nigeria; trustworthy digital identity

Abbreviations: NIN, National Identity Number; NIMC, National Identity Management Commission

Abstract

Nigeria commenced its national foundational digital identity project in 2007 and had enrolled 60 million people by July 2021. The project, led by the National Identity Management Commission (NIMC), seeks to unify the country's public and private functional identity databases, and aims to improve government services and national security. Although the enrolment process had encountered initial challenges such as the absence of enrolment centers in some communities across the country, enrolment for the biometric ID had proceeded without any significant public objection to its objectives. Following the EndSARS protests of October 2020, where youths protesting police violence and perceived poor governance were shot at by government security forces and protesters placed under surveillance, the government announced an updated national identity policy mandating citizens link their National Identity Number (NIN) with their SIM card information. For the first time, significant pockets of resistance arose against the national ID project by sections of the public who perceived the EndSARS violence as signaling a change in government behavior, and the updated ID policy as a mechanism for empowering government surveillance and authoritarianism. The resistance to the ID project marked a shift in public perception which threatens its future. This paper argues that mistrust in government data collection projects grows when data collection is perceived to be increasing government power to the detriment of human rights and freedom. It also puts forward a proposal on how to restore trust within the low-trust environment in Nigeria including the passage of a data protection law and amendments to the NIMC Act and Policies/Regulations, establishing Federated identity providers which give choices to end-users, and delinking the NIN from functional identity databases.

Policy Significance Statement

Projects initiated for developmental outcomes in developing country contexts should place greater emphasis on the human rights impacts of their initiatives. When these projects are national ID projects, concrete technical implementations that make it more difficult to abuse data and that give people agency and choice in the use of IDs need to be instituted. While data protection laws are important in developing countries, they are seldom sufficient to safeguard against data abuses and other human rights deprivations.

1. Introduction

Only 9 years remain to meet the 2030 United Nations' Sustainable Development Goals (SDGs), and in particular SDG 16.9 ("legal identity for all") which aims to "by 2030, provide legal identity for all, including birth registration" (United Nations, 2021). Many governments, particularly in Africa, have taken this goal as the impetus to commence the implementation of digital identity projects, with funding support from international partners (in the case of Nigeria) such as the World Bank, French Development Agency, and the European Investment Bank. This intervention was prompted by the global identification challenge—there are approximately 1 billion people in the world today who face difficulties proving their identities (Desai et al., 2018), and 40% of these individuals are in Africa (World Bank, 2017). This lack of legal identity excludes millions of people from participation in national life in areas such as opening accounts in financial institutions, employment, voting, political participation, and accessing government services and social transfers.

Nigeria, Africa's most populous country and largest economy, commenced its national foundational digital identity project in 2007 and had enrolled 60 million people by July 2021 (NIMC, 2021). The project, led by the National Identity Management Commission (NIMC), seeks to harmonize and integrate public and private functional databases (NIMC, 2019) such as banking information, mobile telephony subscriber information, voter's data, immigration data, and driver's licenses to create a "Universal Identity Infrastructure" for the country (NIMC, 2017) with an aim to improve government services and national security. Funded by the World Bank and others, Nigeria's digital ID project plans to bring coverage of digital ID in Nigeria to 85% of the population and 97.5% of adults by the end of 2027 (World Bank, 2020).

The key feature of Nigeria's digital identity is an 11-digit identifier, the National Identity Number (NIN), which is issued to enrollees after the collection of personal information and biometrics (fingerprints and headshot). The enrolment form contains the full list of information collected from enrollees (NIMC, 2021). A smart digital identity card was initially issued alongside the NIN but was stopped after its inclusion caused the cost of the identity program to exceed budget projections (ID4Africa, 2020). NIMC has now made the NIN the focal point of the national identity scheme, alongside a mobile app available for download on Apple and Android devices. Both the NIN and the mobile app can be used for authentication and verification of identity. Possession of the NIN was made mandatory in January 2019 before individuals can access a range of public and private services such as banking, insurance, pensions, issuance of international passports, driver's license, and payment of taxes (Vanguard, 2018).

Some subnational state governments in Nigeria's 36 state federations have also made the possession of the NIN mandatory to access government services (Ayang, 2021). There are approximately 5,000 enrolment centers across the country (Centre for Internet and Society India, 2021), a number swelled by the mobilization of mobile network operators, partner agencies such as the National Immigration Service, and private vendors. Nigerians resident abroad can also enroll for the NIN in selected locations overseas (NIMC, 2021).

Nigeria's digital identity project was brought into force by the NIMC Act, passed into law by the House of Representatives and the Senate, the arms of the bicameral legislature on May 17, 2007 and May 23, 2007, respectively. In addition to the NIMC Act, Nigeria's digital identity project is also governed by several policies and regulations by NIMC (NIMC, 2021). Nigeria does not have a data protection law, although a data protection bill has been under development for many years. Since its commencement in 2007, there had never been a significant public display of suspicion about the digital identity project, projected through social media. This changed following the EndSars protests of October 2020 in Nigeria (Iwuoha and Aniche, 2021), where youths across Nigeria protested the violence targeted at young people by Nigeria's Police Special Anti-Robbery Squad (SARS) and perceived poor standards of governance. As detailed in the following section, the NIN-SIM policy which shortly followed the EndSars protest heightened suspicion of encroachment on rights to privacy.

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

2. The Onset of Mistrust

The world is facing a pandemic of mistrust. Mistrust in governments, businesses, media, civil society, and other institutions that serve society has become strained in the past few decades (Zuckerman, 2021). One acute manifestation of this problem is the decline in the trust of traditional news sources. Sources of news that had been trusted for decades are succumbing to mistrust as we grapple with a "post-truth" world (Peter, 2017) where "fake news" or "alternative facts" hold sway. The rise in global mistrust in news sources has been clearly felt through the COVID-19 vaccine hesitancy around the world despite persistent media messaging vouching for the safety of vaccines.

Governments are perhaps the most high-profile targets of public mistrust. The 2021 Edelman Trust Barometer (Edelman, 2021), an online survey of over 33,000 respondents in 28 countries (representing 17% of the global population), reports that governments were mistrusted in 13 of 27 countries, including Nigeria, South Africa, Argentina, Colombia, Russia, Spain, Japan, Kenya, Brazil, the United States, the United Kingdom, Mexico, and Ireland. Respondents in a further six countries—France, South Korea, Italy, Thailand, Canada, and Germany—reported neither trust nor mistrust in government, while only nine countries—Australia, Malaysia, the Netherlands, Indonesia, Singapore, United Arab Emirates (UAE) and China—had survey respondents reporting trust in government. This is a recurring trend—an analysis of the data on mistrust in the Edelman Trust Barometer for 4 years from 2018 to 2021 (Edelman, 2018, 2019, 2020, 2021) shows a pattern of mistrust in government. In each year of the survey, the majority of countries surveyed reported a mistrust of government over trust—21 of 28 countries in 2018, 16 of 26 in 2019, 17 of 28 in 2020, and 13 of 27 in 2021. Only five countries in 2018, seven in 2020, six in 2019, and nine in 2021 reported trust in government with the remainder of countries in each yearly survey reporting neither trust nor mistrust (neutral).

An important aspect of the concept of mistrust is that mistrust, especially institutional mistrust, is usually the result of institutions underperforming (Zuckerman, 2021). This is applicable to the situation in Africa, where government services in some countries are either poor or nonexistent. In Africa, citizens have been known to mistrust government messaging on Ebola outbreak prevention methods in the Democratic Republic of Congo (Vinck et al., 2019) and polio vaccines in Northern Nigeria (Grossman et al., 2017) because the government could not be trusted on other things—particularly in the execution of government services. This theme of mistrust stemming from gaps in the social government contract is the theme of this paper and erupted into the tumultuous EndSars protest of October 2020 in Nigeria.

3. The EndSars Protest

The EndSars protest of October 2020 was a watershed moment in the history of Nigeria. For the first time, the nation's youths were unified in action to protest targeted violence by the security services and perceived poor governance by a ruling class which included few of their generation (Iwuoha and Aniche, 2021). Nigeria's population, like elsewhere in Africa, is very young. The percentage of the population of individuals 0–14 years is 43% (World Bank, 2021a,b,c).

With a youth unemployment rate of 42.5% (National Bureau of Statistics, 2021), there has always been a deep-seated resentment among Nigeria's youth that they had been given the raw end of the deal by a country that had largely ignored them. Today, Nigeria is classified as the country with the largest number of people living in extreme poverty in the world (Slater, 2018), yet in this dire context, thousands of youths have labored to forge out a living through engagement in sectors such as technology, where Nigeria's youth have carved out an international reputation in technology hubs across the country (Ramachandran et al., 2019). Through crafts such as coding, website development, and app development many Nigerian youths have defied the poor working environment in the country. Unfortunately, Nigeria also has a cybercrime problem (Aransiola and Asindemade, 2011; Ibrahim, 2016), and in tackling the problem of cybercrime, security agencies have often painted cybercriminals in Nigeria's cities with the same brush as the teeming population of youth technology entrepreneurs (Okunoye, 2021). They are in the same generation, carry the same technology devices, and often have the same lifestyle—while cybercriminals

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

might have access to easy money through proceeds of fraud, technology entrepreneurs have incomes that make for comfortable lifestyles. This targeting by security services of the young army which populate Nigeria's booming technology sector, leading to harassment, arrests, and deaths sparked the EndSars protest and led to a bigger rally against perceived poor governance in Nigeria.

The EndSars protest has changed Nigeria, bringing to the fore a new generation of Nigerian youth who have demonstrated they will not be content with the status quo (BBC, 2020). Having never witnessed such a sustained, determined, and spontaneous protest by youth calling it to account, the Nigerian government responded by commencing negotiations with the youth and announcing the reopening of tertiary institutions—a tactic to diminish the number of protestors. Despite ongoing negotiations, the protesters were not convinced of the sincerity of the government to meet all their demands—which included a genuine and thorough disbanding of the police Special Anti-Robbery Squad (SARS). When protests continued, on the night of October 20, 2020 in Lekki Nigeria, the focal point of the protest, armed soldiers opened fire on unarmed protesters leading to loss of many lives and injuries in an incident that sparked major international outrage with politicians and leaders across the world reacting to the violence used against unarmed protesters (DW, 2020).

4. Updated ID Policy

The relationship that end-users have with the government has a strong influence on their behavior and attitudes toward identity (Wilson, 2019). This was perfectly exemplified by the turn of events in Nigeria leading to the first major resistance to Nigeria's digital ID project, following the government crackdown of EndSars protesters on October 20, 2020. Immediately following the violent government response, bank accounts of individuals perceived to be leaders of the protest were frozen (Human Rights Watch, 2020), although it was clear this was a truly organic and spontaneous reaction of young people across the country. An EndSars organizer was prevented from traveling, having been placed on no-fly lists monitored at the country's border exits (Kabir, 2020). Businesses perceived to be supportive of the protests were also targeted, including Flutterwave, a technology start-up founded by young Nigerians which had a few weeks earlier been valued at over US$1 bn (Adebowale, 2020). Flutterwave represented the kind of endeavor young Nigerians in the technology sector were engaged in and it was active as a payment platform during the EndSars protests. After having been shot at, and had their freedom curtailed for participating in peaceful protests, the aftermath of the EndSars protests led many young Nigerians to feel disillusioned about Nigeria. Many openly expressed their desire to leave the country (Jones, 2021).

Three months after the EndSars protests, the Nigerian government through the Nigerian Communications Commission, the Communications Regulator, released an updated National Identity Policy working closely with NIMC (NCC, 2020). Central to this revised policy was the requirement that people who had enrolled for the NIN link their subscriber identifier module (SIM) card with their NIN through an online link or the 'Unstructured Supplementary Service Data' (USSD) code *346# dialed on any mobile network in Nigeria (a USSD code is a Global System for Mobile Communications (GSM) protocol that is used for information services). The policy also required data on citizens' International Mobile Equipment Identifier (IMEI) numbers. For the first time since the start of the national ID project in 2007, there was significant and vocal resistance (Iruoma, 2021) to the ID project from among young people who read the updated policy and its requirements as means to strengthen the powers of government surveillance and restrict their freedom.

Nigeria's youth represent the largest segment of the population (World Bank, 2021a,b,c) and significant resistance within this demographic does not bode well for plans to ensure inclusivity and adoption of the country's ID project. In retrospect, given that the relationship that end-users have with the government has a strong influence on their behavior and attitudes towards identity (Wilson, 2019), and institutional mistrust is strongly linked with institutions such as government underperforming (Zuckerman, 2021), it is probable that if Nigeria's youth unemployment rate were not so high (42.5%) and youths were otherwise profitably employed and engaged within the economy, the resistance demonstrated towards the national ID might have been much less, and the EndSars protests might not have been as severe. The link between

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

the abject condition of the country's youth and the raging EndSars protests was tacitly acknowledged by the government, which quickly moved to reach an arrangement with the academic staff union of the nation's Universities who had been on a strike in protest of poor working conditions (Olufemi, 2020). The Universities were thereby ordered to reopen, and students were urged to return to their campuses, in a bid to drain the fervor of the protests.

Another facet of the institutional mistrust and societal tensions around digital identity projects stems from the perceived legality of the actions of implementers and administrators of the project (Manby, 2021). In the UN SDG 16.9 plan to "provide *legal* identity for all" for instance, the rule of law and legality is implied as core tenets of any identity regime. The 1948 Universal Declaration of Human Rights (UDHR) and the 1966 International Covenant on Civil and Political Rights (ICCPR) are among the international human rights standards establishing the right to an identity, thus giving the provision of identity a footing within established international legal frameworks. Although Nigeria's national identity project is backed by law and extensive policies, the deep mistrust and hesitation towards the government ID policy such as the NIN-SIM linkage discussed above, which concentrates power in the hands of the government, cannot be divorced from observations such as the government ignoring court orders and, in some instances, seemingly treating the Judiciary with disdain (Kabir, 2019; Olaniyan, 2019).

This paper also endeavors to make a distinction between "trust" and "trustworthiness" in digital identity systems, buttressing the work of researchers, some of whom have rightly expressed that a digital identity system might be trusted even when it is not trustworthy (Maple, 2021). In the context of digital identity systems, "trust" can be defined as a belief in the integrity of the system, while "trustworthiness" refers to the extent to which it is deserving of trust (Maple et al., 2021). That is, although governments might strive to win the trust of the public in national identity systems through consistent messaging by the specific ministry in charge of implementing the ID, when internationally acknowledged technical pillars underpinning the trustworthiness of the ID system are lacking or poorly implemented, it is clear they do not deserve the trust they seek to gain. Prominent research and multilateral organizations have worked to establish the pillars of what might constitute a trustworthy digital identity system.

For instance, a group of 28 international organizations including the World Bank, the United Nations Development Programme (UNDP), and the International Telecommunications Union (ITU), have endorsed "Principles on Identification" (Desai and Clark, 2021; World Bank, 2021a,b,c). These 10 principles consist of three pillars, inclusion, design, and governance which make up the 10 principles defined below (Table 1).

Similarly, the Alan Turing Institute (Maple et al., 2021) has identified what constitutes the pillars of Trustworthy digital identity, defining six facets of trustworthy digital identity systems as:

Table 1. *Principles of identification*

Principles	
Inclusion	1. Ensure universal access for individuals, free from discrimination
	2. Remove barriers to access and use
Design	3. Establish a trusted—unique, secure, and accurate—identity
	4. Create a responsive and interoperable platform
	5. Use open standards and prevent vendor and technology lock-in
	6. Protect privacy and agency through system design
	7. Plan for financial and operational sustainability
Governance	8. Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework
	9. Establish clear institutional mandates and accountability
	10. Enforce legal and trust frameworks through independent oversight and adjudication of grievances

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

1. Security: "The protection of data, information and systems against unauthorised access or modification whether in storage, processing, or transit and against denial of service to authorised entities."
2. Privacy: "Ensure that personal and sensitive information transmitted, processed, and shared is treated privately, in adherence to legal and regulatory restrictions governing its use".
3. Robustness: "The ability of the system to continue functioning in the presence of internal and external challenges without fundamental or drastic changes to its original operations or state".
4. Ethics: "Ensure transparent, responsible, and auditable operations throughout the whole lifecycle of data and information management in systems whilst enabling user empowerment into this process".
5. Reliability: "The ability of the system to perform in a consistent and expected way during a period of time in which it adheres to its performance specifications adequately".
6. Resiliency: "The ability of the system to adjust to internal and external conditions by adapting its operations to ensure the continuation of expected service under these new conditions."

The six facets of trustworthy digital identity further consist of 16 facet attributes and 49 features and mechanisms (Maple et al., 2021).

Nevertheless, as Manby (2021) notes, the organizations that shape digital identity research and policy sometimes have only limited enforcing power to ensure that these Trustworthy ID principles are indeed implemented in specific country contexts. For example, the World Bank, a major funder of Nigeria's national ID, has made several recommendations (some listed in the section below) on how to improve the trustworthiness of the system.

It is true that a national digital identity system might be trusted by its users because of effective government messaging to that effect, even though it is not trustworthy as defined by the parameters above. However, the converse might also be true. A trustworthy digital identity system, which has made significant progress towards implementing the pillars of trustworthiness, might still be untrusted by many users in a country because of the fraught relationship people have with the government, reinforcing the observation that the relationship that end-users of identity have with government shapes the uptake of digital identity (Wilson, 2019).

In Nigeria this effect is measurable. Data from the National Bureau of Statistics (NBS) shows a decline of over 12 million active Internet subscribers in Nigeria from Q4 2020 to Q4 2021 (National Bureau of Statistics, 2022). Many were people who were removed from the network because they refused to comply with the government NIN-SIM directive. A perspective from the government is that these individuals are "criminals" who refuse to be registered by the government because they do not want to be "regularized" (Okon, 2022). However, it is unlikely that such a significant decrease of 12 million (7.99%) Internet connections can be attributed solely to individuals trying to evade the law. Government policy has been the source of some public discomfort (Iruoma, 2021) and government mistrust is a possible explanation as to why there was a reduction in Internet subscribers.

This difficult citizen-government relationship which creates scenarios such as the EndSars protest and its aftermath, is common with fledgling democracies where the rule of law and accountability need to be strengthened. Admittedly, this might be a long-term project. In such low trust environments, however, it becomes imperative that at least the basics—the pillars of trustworthiness—are fully and not partially covered, in order to restore trust.

5. Restoring Trust

At the core of the mistrust around Nigeria's digital IDs is the question of whether IDs will be a vehicle of good governance reflected in the respect of fundamental human rights and diverse viewpoints, or rather an instrument of oppression, surveillance, and clampdown on human rights. This reflects the global debate and tension on the use of data and technology in the aid of international development (Weitzberg et al., 2021). That is, do data technology projects such as national ID projects serve the interests of "data

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

justice"—respecting human rights and improving the human condition, or instead "data injustice"—empowering exploitation and human rights violations (Dalton et al., 2016; Iliadis and Federica, 2016; Taylor, 2017)? The goal of the national identity project as stated by NIMC is to serve as a vehicle of national development through enabling the delivery of social services, stamping out public waste, and tackling insecurity. Nevertheless, the events narrated above heightened the perception that there was a link between the updated National ID policy and an intent for government surveillance and clampdown on civil freedoms. Those perceptions stemmed from the current practice of Nigeria's democracy—which has made a lot of progress, yet still has some way to go to reflect the best ideals of democratic practice. While solving democratic ills might be a long-term project, there are specific short-term design choices that might be implemented to restore trust in digital identity projects in emerging democratic contexts such as Nigeria.

5.1. The passage of a data protection law and amendments to the NIMC Act and Policies/Regulations

Perhaps the singular most important step which might be taken to improve trust around Nigeria's digital ID is the passage of a data privacy law, and specific amendments to the NIMC Act and some of its accompanying policies. Although it has arguably the largest digital identity project in Africa, catering for Africa's largest population of over 200 million people, Nigeria does not currently have a data protection law. Nigeria's data protection provisions include section 37 of the 1999 Constitution (amended) which guarantees the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications. The provisions of section 37 of the constitution have not been reflected in a corresponding national legislation; hence, the applicability and coverage of its provisions is unclear (World Bank, 2020). It also includes legislation crafted for specific sectors of national life (hence with restricted scope) such as the Child's Right Act, Freedom of Information Act, Cybercrimes Act, and the Credit Reporting Act. Several regulations by agencies of the Federal government also provide limited, sectoral protections for privacy. These include the Central Bank's Consumer Framework, the Nigerian Communications Commission Regulations, and the Nigeria Data Protection Regulation created by the National Information Technology Development Agency (NITDA). Fortunately, progress is being made towards the attainment of a data protection law. Nigeria's data protection bill is currently before the Nigerian Senate, where it is expected to pass at the end of 2022 (Olatunji, 2022).

In addition to the passage of the data protection law, there are several data protection defeating clauses in the NIMC Act, and its accompanying policies/regulations:

1. Section 26 of the NIMC Act allows the sharing of ID data of registered persons with third parties without their consent. The conditions under which data can be shared are vague and open the door for use of data for state surveillance—precisely the fear that has spurred some public mistrust in the ID project.
2. The Access to Register Information on the National Identity Database Regulation expands on the data sharing harms of Section 26 of the NIMC Act above.
3. Section 3(2) of the Registration of Persons and Contents of the National Identity Database Regulations 2017 confers the ownership of registered person's ID data on the Federal government. ID data are to be treated as classified material under the Official Secrets Act.

5.2. Federated databases: Decentralized systems providing choices

An important characteristic of trusted ID systems is the federation of identity providers that provide choices to users (Whitley, 2018; Mozilla, 2020; World Bank, 2021). An example of a federation in national ID systems is found in the United Kingdom (UK), which has no single foundational ID system except for a civil registry. Under the UK system, people employ a combination of several identity credentials such as driving licenses, passports, and birth certificates to prove their identities for public and private transactions using the GOV.UK Verify platform for authentication.

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

The UK represents one of many nations including the United States, France, Australia, and Canada where centralized ID databases that mandate the use of a national ID card were resisted (Mozilla, 2020). These nations are among the most advanced democracies in the world with high human rights standards including data protection frameworks. Yet, despite these data protection safeguards, there seems to be little enthusiasm for technical implementations that rely on the centralization of citizen data (AccessNow, 2018).

According to the World Bank, a rationale for centralized ID databases like that of Nigeria's national system is that the country's previous identity landscape was fragmented, disconnected, and duplicative with at least 13 different Federal governments and about three state government agencies running identity programs (World Bank, 2020), some with biometric data. Some of these Federal government agencies include the Nigerian Immigration Service which issues passports, National Population Commission which manages the civil registry, the Independent National Electoral Commission (INEC) which manages the voter's registry, and the Federal Road Safety Commission (FRSC) which issues driver's licenses. According to a 2015 World Bank estimate, Nigeria might have spent a wasteful US$4.3 billion to implement this fragmented ID system (World Bank, 2020).

The fragmented nature of Nigeria's identity system was the rationale for mandating the compulsory use of the national ID card as the sole identity provider (NIMC, 2007, 2019). However, perhaps the best response to a fragmented identification landscape where at least 16 IDs held sway in the country is probably not a unified identity landscape where only one ID is used. The former is a failure of coordination and planning within different segments of government who were not under coercion to use this fragmented system, while the latter is perhaps a hurried reaction to the former. This replaces one problem—disorderliness and waste, with a different type of problem—centralized control and an absence of choice and agency for people in the use of IDs. National ID practices like those described above in the United Kingdom where the country functions without a centralized ID system, and a diverse but limited set of IDs cater to a population might be examples to draw from. For Nigeria, what if between birth registration, passport, driver's license, bank verification number (BVN)/pension number, national health insurance number, SIM registration, and voter's registration we create an identity ecosystem similar to the UK's GOV.UK where people have choices and agency in the appropriation of IDs? Many of the existing ID systems in Nigeria already collect rich and detailed information, including unique biometric identifiers, and boast enrolment figures exceeding or similar to, the figures for the national ID. Finding the right balance of number of approved IDs in the national ecosystem (of which the national ID is a part) is key. The national ID can serve as part of a whole ecosystem of identity, rather than the sole identity.

The enrolment data from the current national ID program suggest the correctness of this ID strategy. To enroll for Nigeria's national ID, an individual must ordinarily provide any of 19 feeder identification documents (NIMC, 2021), five of which are described in Table 2. Data from enrolment suggest that the majority of those enrolled so far are individuals who already had one of these feeder IDs and NIMC efforts are now directed at a second phase of enrolment specifically targeted at those without these feeder documents, by allowing them to present alternative means of proving their identities (ID4Africa, 2021a,b; Mojeed, 2021).

Federated and decentralized ID systems present practical security and privacy advantages. One, they do not present a single point of failure in the event of a cyber breach. An attacker who gains access to a database is limited to only the data contained therein and cannot access other records. The importance of this feature was demonstrated in 2021 when hackers gained access to the Argentinian national ID registry (ID4Africa, 2021a,b). They also demonstrate some robustness and resiliency—a technical downtime in one system does not ground the entire identity ecosystem. The usefulness of this feature was demonstrated in February 2022 when a technical glitch occurred in the government IT services provider which hosts the servers of NIMC (Okunoye, 2022). This left many individuals and organizations needing to access NIN verification services stranded for over 10 days, with no effective alternatives.

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

Table 2. *Enrolment figures or coverage of selected IDs in Nigeria*

s/no	ID document	ID provider	Figure or %	Biometrics?	Comments
1.	Birth certificate	National Population Commission	43%[a]	No	Population of 200 million
2.	Voter's registration	Independent National Electoral Commission	84 million[b]	Yes	2019 elections
3.	Driver's license	Federal Road Safety Commission	11 million[c]	Yes	Proxy from number of cars[d]
4.	SIM registration	Nigerian Communication Commission	190 million[e]	Yes	
5.	Bank Verification Number (BVN)	Central Bank of Nigeria and Banks	51 million[f]	Yes	
6.	National ID	National Identity Management Commission	60 million[g]	Yes	

[a]https://www.unicef.org/nigeria/press-releases/only-43-cent-nigerian-childrens-births-registered-unicef;
[b]https://www.electionguide.org/countries/id/158/;
[c]https://www.nigerianstat.gov.ng/pdfuploads/Road_Transport_Data_-_Q2_2018.pdf;
[d]Many drivers lack licenses, and other license holders have multiple cars;
[e]https://www.ncc.gov.ng/statistics-reports/industry-overview#gsm;
[f]https://nibss-plc.com.ng/services/bvn;
[g]https://nimc.gov.ng/nimc-reaches-more-than-sixty-million-60-unique-nin-records/.

5.3. Delinking National Identity Number from functional databases

An important design choice for Nigeria's national ID is the "harmonization" of the national ID with existing ID card schemes in the country (Section 15 of the NIMC Act). It is claimed this aims to cut fraud and improve security. What it really does is give the government powers of centralized surveillance over citizens' data. In the case of Nigeria, many of these functional IDs to be "harmonized" with the national identity data to collect unique biometric information before the registration of individuals. The use of biometrics is becoming widespread in Nigeria to the point that even social protection programs in Nigeria such as school meals programs collect biometric information (Hersey, 2021). Unique biometrics are already a trusted efficient security measure and removes the possibility of fraud—the stated aims of harmonizing all functional identity data with the national identity. What linking the national ID with these databases does is to give the government an instant, comprehensive view of citizens' data, thereby increasing their power of surveillance, which breeds mistrust in an already low-trust environment.

It is interesting to note that two of the reforms suggested—the passage of a data protection law and the amendment (of section 27) of the NIMC Act to codify the removal of the mandatory usage of the national ID (but not the provision of alternative ID choices)—are compulsory reforms demanded (World Bank, 2020) before the complete disbursement of funding from the World Bank, a major funder of Nigeria's identity project. The former is in progress, with the law expected before the end of 2022 (Olatunji, 2022). It remains to be seen what other funder-required reforms will be implemented. For example, it is not clear how the World Bank's requirement that the use of the national ID card should not be made compulsory without at the same time ensuring that other ID alternatives are legitimized in a context where the national ID is gradually being positioned to be the sole identity document.

5.4 IDs for all remain a worthy goal

This paper acknowledges the importance of the goals of the identification for development movement. There are 1 billion people in the world without proof of identification, and over half reside in Africa (Desai et al., 2018). Nevertheless, perhaps a rethink of the strategy towards achieving this is needed in developing

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

country contexts, taking into account peculiar local contexts. The international support toward strengthening the civil registration and vital statistics in developing countries ought to continue and should form the basis of foundational identities—like it is in developed countries. While work on this continues annually, the shortfalls in identity cover can be pursued with national ID programs—but this should focus instead on the segment of the population without any IDs, where social grant programs can be crafted to encourage their participation because they otherwise do not possess any feeder documents (LeVan et al., 2019). They also tend to live in marginalized communities where resentment towards participation in government projects is high because of a fraught relationship with the government which is perceived to have failed in the provision of services. The demographic without any feeder identity documents are precisely the group needing the national ID in the first place, toward achieving the aim of IDs for all as per SDG 16.9 and of international development partners such as the World Bank.

Thus national ID, birth registration, and a unique set of trusted IDs chosen by country planners can then serve as the national ID ecosystem. Mandating a compulsory national ID causes exclusion, and a centralized ID database which links data across several databases increases the government's powers of surveillance which can breed mistrust in low-trust environments.

6. Conclusion

More than 40% of people lacking IDs in the world live in Africa (World Bank, 2017), and the objectives of development partners in providing identification to people lacking them are laudable. Nevertheless, many of these people also reside in sociopolitical contexts where the rule of law is still contested and where the Judiciary is weak. Therefore, the "social risks" of misuse of data acknowledged by partners such as the World Bank (2020) in countries where they fund ID projects cannot be mitigated only by the existence of data protection laws—in many of these countries laws are sometimes not enough to prevent data abuse. Concrete, technical implementations that make it more difficult to abuse data are critically important. While the provision of legal identity for all by 2030 (United Nations, 2021) is an important United Nations sustainable development goal (goal 16.9), human rights considerations are probably more weighty and foundational values that undergird human existence, and should not be watered down or threatened by the pursuit of developmental objectives. In Nigeria in particular, a reorientation of the national ID program to those without feeder IDs to attain the goals of IDs for all, and a commitment to using the NIN as part of a federated ID ecosystem without extensive inter-linking and centralization of citizen data are key to creating such an ID ecosystem.

Acknowledgments. The author is grateful for the opportunity granted by the Alan Turing Institute, London, United Kingdom to present (Okunoye, 2021) some of the ideas presented in this paper at the Turing Trustworthy Digital Identity Conference in September 2021.

Funding Statement. This work received no specific grant from any funding agency, commercial, or not-for-profit sectors.

Competing Interests. The author declares no competing interests exist.

Author Contributions. Conceptualization: B.O.; Data curation: B.O.; Formal analysis: B.O.; Investigation: B.O.; Methodology: B.O.; Project administration: B.O.

Data Availability Statement. Data availability is not applicable to this article as no new data were created or analyzed in this study.

References

AccessNow (2018) *National Digital Identity Programmes: What Next?* AccessNow.

Adebowale A (2020) *#ENDSARS: Central Bank of Nigeria Allegedly Summons Flutterwave, Cuts Off Donation Accounts.* Available at https://technext.ng/2020/10/13/endsars-central-bank-of-nigeria-allegedly-summons-flutterwave-cuts-off-donation-bank-accounts/. (accessed 17 March 2022).

Aransiola JO and Asindemade SO (2011) Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. *Cyberpsychology, Behavior and Social Networking 14*, 759–763. https://doi.org10.1089/cyber.2010.0307

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

Ayang M (2021) Nigerian State makes Digital ID Numbers Mandatory to Access Government Services. Available at https://www.biometricupdate.com/202103/nigerian-state-makes-digital-id-numbers-mandatory-to-access-government-services.

BBC (2020) *How the End Sars Protests Have Changed Nigeria Forever.* Available at https://www.bbc.com/news/world-africa-54662986.

Centre for Internet and Society India (2021) *Nigeria's Digital ID: The Blueprint.* Available at https://www.youtube.com/watch?v=nlSfw2XW1s8.

Dalton CM, **Taylor L and Thatcher J** (2016) Critical data studies: A dialog on data and space. *Big Data and Society 3*, 1–9.

Desai V and Clark J (2021) *10 Principles for Good ID: A 2021 Refresh.* Available at https://blogs.worldbank.org/voices/10-principles-good-id-2021-refresh.

Desai V, **Diofasi A and Lu J** (2018) *The Global Identification Challenge: Who are the 1 Billion People Without Proof of Identity?*. Accessed 17/03/2022 Available at https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity?__cf_chl_captcha_tk__=pmd_bwOnsk5lCPzgeVyalocY0aBH.U9djbfAsg117ev6I1s-1632124517-0-gqNtZGzNAyWjcnBszQvl.

DW (2020) Nigeria: UN Slams 'Brutality' Against #EndSARS Protesters. Available at https://www.dw.com/en/nigeria-un-slams-brutality-against-endsars-protesters/a-55349495.

Edelman (2018) *Edelman Trust Barometer 2018*. Chicago, IL: Edelman.

Edelman (2019) *Edelman Trust Barometer.* Chicago, IL: Edelman.

Edelman (2020) *Edelman Trust Barometer.* Chicago, IL: Edelman.

Edelman (2021) *Edelman Trust Barometer 2021*. Chicago, IL: Edelman.

Grossman S, **Phillips J and Rosenzweig LR** (2017) Opportunistic accountability: State-society bargaining over shared interests. *Comparative Political Studies 51*, 979–1011.

Hersey F (2021). *Nigeria Collects Biometrics of Elementary School Children for Meal Program.* Available at https://www.biometricupdate.com/202110/nigeria-collects-biometrics-of-elementary-school-children-for-meal-program.

Human Rights Watch (2020) *Nigeria: Punitive Financial Moves Against Protesters.* Available at https://www.hrw.org/news/2020/11/13/nigeria-punitive-financial-moves-against-protesters.

Ibrahim S (2016) Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice 47*, 44–57.

ID4Africa (2020) *Nigeria's Identity Ecosystem [video].* Available at https://www.youtube.com/watch?v=OgcKzQ8I7_U&t=4425s.

ID4Africa (2021a) EP19: Nigeria & Rwanda ID Systems + International ID Day Celebration & Competition. Available at https://www.youtube.com/watch?v=6FXqp7A1bB0&t=4632s.

ID4Africa (2021b) EP24: The Dark Side of Identity: Mitigating the Risks (PT 2): A Data-Centric Approach. Available at https://www.youtube.com/watch?v=zJ7oIV1T5HA.

Iruoma K (2021) ANALYSIS-Got Your Number: Privacy Concerns Hobble Nigeria's Digital ID Push. Available at https://www.reuters.com/article/nigeria-tech-rights-idUSL8N2OW2CJ.

Iwuoha VC and Aniche ET (2021) Protests and blood on the streets: Repressive state, police brutality and #EndSARS protest in Nigeria. *Security Journal*. https://doi.org/10.1057/s41284-021-00316-z

Jones M (2021) Nigeria's #EndSars Protest: What Happened Next? Available at https://www.bbc.com/news/world-africa-58817690.

Kabir A (2019) ANALYSIS: SSS: Nigeria's Security Agency Notorious for Disobeying Court Orders. Available at https://www.premiumtimesng.com/news/headlines/355037-analysis-sss-nigerias-security-agency-notorious-for-disobeying-court-orders.html.

Kabir A (2020) #EndSARS Protest Promoter Stopped from Traveling Abroad. Available at https://www.premiumtimesng.com/news/more-news/424513-endsars-protest-promoter-stopped-from-traveling-abroad.html.

LeVan C, **Hassan IO**, **Isumonah VA**, **Kwaja CM**, **Momale SB**, **Nwankwor CO and Okenyodo K** (2019) *Study on Marginalized Groups in the Context of ID in Nigeria National Identification for Development (ID4D) Project*. Washington DC: World Bank.

lliadis A and Federica R (2016) Critical data studies: An introduction. *Big Data & Society 3*, 1–7.

Manby B (2021) *SDGs and Legal Identity for All: First, Do No Harm*. Elsevier: World Development, pp. 105343–105354.

Maple C (2021) Exploring Over-Reliance on Blind Trust in Digital IDs. Available at https://www.turing.ac.uk/blog/exploring-over-reliance-blind-trust-digital-ids.

Maple C, **Epiphaniou G and Gurukumar N** (2021) *Facets of Trustworthiness in Digital Identity Systems*. London: The Alan Turing Institute.

Mojeed A (2021) BVN Generated NIN Must be Verified to Access NIMC Mobile App – Official. Available at https://www.premiumtimesng.com/news/more-news/436439-bvn-generated-nin-must-be-verified-to-access-nimc-mobile-app-official.html.

Mozilla (2020) Bringing Openess to Identity: Technical and Policy Choices for Open National ID Systems.

National Bureau of Statistics (2021) Unemployment Statistics. Available at https://www.nigerianstat.gov.ng/.

National Bureau of Statistics (2022) *Telecoms Data: Active Voice and Internet Per State, Porting and Tariff Information (Q2,Q3, Q4 2021).* Available at https://nigerianstat.gov.ng/elibrary/read/1241133.

NCC (2020) Press Statement: Implementation Of New Sim Registration Rules. Available at https://www.ncc.gov.ng/media-centre/news-headlines/928-press-statement-implementation-of-new-sim-registration-rules.

NIMC (2007) *National Identity Management Commission Act*. New Delhi: NIMC.

NIMC (2017) *NIMC.* Available at https://nimc.gov.ng/docs/harmonization_policy.pdf.

NIMC (2021a) NIMC Enrolment Centres. Available at https://nimc.gov.ng/nimc-enrolment-centres/.

https://doi.org/10.1017/dap.2022.29 Published online by Cambridge University Press

NIMC (2021b) Policies. Available at https://nimc.gov.ng/policies/.
NIMC (2019) We are Committed to Providing a Unified Database – NIMC. Available at https://nimc.gov.ng/we-are-committed-to-providing-a-unified-database-nimc/.
NIMC (2021c) Enrolment Dashboard July 2021. Available at https://nimc.gov.ng/enrolment-dashboard-july-2021/.
NIMC (2021d) Enrolment Form. Available at https://nimc.gov.ng/enrolment-form/.
NIMC (2021e) *How to Enrol (Adults): Supporting Documents*. New Delhi: NIMC.
Okon D (2022) Network Shutdowns, NIN-SIM policy… How Regulations Impacted Telecoms Sector in 2021. Available at https://www.thecable.ng/network-shutdowns-nin-sim-policy-how-regulations-impacted-telecoms-sector-in-2021.
Okunoye B (2021a) Mistrust of Government in Context of Repressive States as a Driver of Slow Acceptance of Digital IDs. Available at https://www.youtube.com/watch?v=s9855H9sZN4&list=PLuD_SqLtxSdVy8meO_ezV9l89Q9Gg8q6p&index=7.
Okunoye B (2021b) Technology and Youth Represent Nigeria's Path Out of the Woods. Available at https://www.cfr.org/blog/technology-and-youth-represent-nigerias-path-out-woods?utm_medium=social_share&utm_source=tw.
Okunoye B (2022) #GoodID Lessons: Why Nigeria Needs More Than the NIN. Available at https://www.africaportal.org/features/goodid-lessons-why-nigeria-needs-more-nin/.
Olaniyan K (2019) Rule of Law? What Rule of Law? Available at https://mg.co.za/article/2019-11-22-00-rule-of-law-what-rule-of-law/.
Olatunji S (2022) Data Protection Bill'll be Passed Before Dec –Olatunji. Available at https://punchng.com/data-protection-billll-be-passed-before-dec-olatunji/.
Olufemi A (2020) ASUU Strike Allows Students to Join #EndSARS Protest — FG. Available at https://www.premiumtimesng.com/news/top-news/421171-asuu-strike-allows-students-to-join-endsars-protest-fg.html.
Peter MA (2017) Education in a post-truth world. *Educational Philosophy and Theory 49*, 563–566.
Ramachandran V, **Obado-Joel FR**, **Masood JS and Omakwu B** (2019) *The New Economy of Africa: Opportunities for Nigeria's Emerging Technology Sector*. Washington DC: Center for Global Development.
Slater J (2018) India is No Longer Home to the Largest Number of Poor People in the World. Nigeria Is. Available at 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/.
Taylor L (2017) What Is data justice? The case of connecting digital rights and freedoms globally. *Big Data & Society 4*, 1–14.
United Nations (2021) Sustainable Development Goals. Available at https://sdgs.un.org/goals/goal16.
Vanguard (2018) Mandatory Use of National ID Numbers BEGINS January 2019. Available at https://www.vanguardngr.com/2018/09/mandatory-use-of-national-id-numbers-begins-january-2019/.
Vinck P, **Pham PN**, **Bindu KK**, **Bedford J and Nilles EJ** (2019) Institutional trust and misinformation in the response to the 2018–19 Ebola outbreak in North Kivu, DR Congo: A population-based survey. *Lancet Infectious Diseases 19*, 529–536.
Weitzberg K, **Cheesman M**, **Martin A and Schoemaker E** (2021) Between surveillance and recognition: Rethinking digital identity in aid. *Big Data & Society 8*, 1–7.
Whitley EA (2018) *Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach.* Centre for Global Development.
Wilson M (2019) *Identity and the Global Poor*. London: GSMA.
World Bank (2017) *The State of Identification Systems in Africa: Country Briefs*. Washington DC: World Bank Group.
World Bank (2020) *Project Appraisal Document on a Proposed Credit for the Digital Identification for Development Project*. Washington DC: World Bank.
World Bank (2021a) Population Ages 0–14 (% of Total Population) - Nigeria. Available at https://data.worldbank.org/indicator/SP.POP.0014.TO.ZS?locations=NG.
World Bank (2021b) Practitioner's Guide: Authentication Mechanisms. Available at https://id4d.worldbank.org/guide/authentication-mechanisms.
World Bank (2021c) *Principles on Identification for Sustainable Development: Toward the Digital Age (English)*. Washington DC: World Bank.
Zuckerman E (2021) *Mistrust: Why Losing Faith in Institutions Provides the Tools to Transform them*. New York: W. W. Norton & Company.

Cite this article: Okunoye B (2022). Mistrust of government within authoritarian states hindering user acceptance and adoption of digital IDs in Africa: The Nigerian context. *Data & Policy*, 4: e37. doi:10.1017/dap.2022.29