Journal of Responsible Technology 11 (2022) 100039

Contents lists available at ScienceDirect

Journal of Responsible Technology

journal homepage: www.sciencedirect.com/journal/journal-of-responsible-technology

Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural concerns

Damian Eke [a,*], Ridwan Oloyede [b], Paschal Ochang [a], Favour Borokini [c], Mercy Adeyeye [d], Lebura Sorbarikor [e], Bamidele Wale-Oshinowo [f], Simisola Akintoye [g]

[a] Centre for Computing and Social Responsibility, De Montfort University, Leicester, United Kingdom
[b] Tech Hive Advisory, Nigeria
[c] Policy, Uganda
[d] Dept. of Entrepreneurship and Business Studies, Federal University of Technology, Minna, Nigeria
[e] Rivers State University, Port Harcourt, Nigeria
[f] University of Lagos, Nigeria
[g] Centre for Law, Justice and Society, De Montfort University, Leicester, United Kingdom

ARTICLE INFO

Keywords:
Digital identification
Identity management
Nigeria
Ethics
Socio-cultural concerns
eID

ABSTRACT

National digital identity management systems have gained traction as a critical tool for inclusion of citizens in the increasingly digitised public services. With the help of the World Bank, countries around the world are committing to building and promoting digital identification systems to improve development outcomes as part of the Identity for development initiative (ID4D). One of those countries is Nigeria, which is building a national ID management database for its over 100 million residents. However, there are privacy, security, human rights, ethics and socio-cultural implications associated with the design and scaling of such a system at a national level. Through a mixed method approach, this paper identifies some of these concerns and categorises which ones Nigerians are most worried about. It provides an empirically sound perspective around centralised national electronic identity (eID) management system, public trust and responsible data governance, and offers recommendations on enhancing privacy, security and trustworthiness of the digital infrastructure for identity management in Nigeria.

1. Introduction

In the Global North (countries located in the Northern hemisphere), digital identification systems are often fundamental to many aspects of the society including security, education, employment, financial services, election and welfare services (Gelb & Clark, 2013). Mostly driven by advancements in technology, since the events of 9/11, ID systems have become integral to national surveillance and security strategies for the USA and many countries in Europe (Lyon, 2009). In the past decade, the provision of legal identity for all (including birth registration) has become an agenda shared by the global community as part of the UN's sustainable development goal (SDG 16.9) (United Nations, 2015). Countries in the Global South (countries located in the southern hemisphere) including Nigeria are beginning to increase efforts towards developing robust identification management systems that can improve the delivery of public and private services for development.

In 2007, the Nigerian National Identity Management Commission (NIMC) was established under the NIMC Act No. 23 of 2007, and given the mandate "to own, operate, maintain and manage the National Identity Database in Nigeria, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to those who are citizens of Nigeria as well as others legally residing within the country'' (National Identity Management Commission Act 2007). The underlying goal is to create a "national system of identifying all citizens in order to accomplish the legitimate business of government – law enforcement, intelligence, social and economic development.''(NIMC, 2005) Since then, Nigeria has developed a number of identification programs at national and state levels. At least, 13 federal agencies and many state agencies currently offer identification services in Nigeria. For example, in partnership with the private sector, different agencies provide ID services such as the Bank Verification Number (BVN), National Identification Number (NIN),

* Corresponding author.
E-mail address: damian.eke@dmu.ac.uk (D. Eke).

https://doi.org/10.1016/j.jrt.2022.100039

Available online 16 July 2022

Voter's ID Card, SIM card registration, driver's licence and International Passport. This paints a picture of a fragmented ecosystem creating different databases of citizens data in unsecured silos. However, the NIMC's electronic ID (eID) strategy focuses on streamlining the fractured ID ecosystem in Nigeria to create a central system to provide the citizens with "social safety net, financial inclusion, digital payments, employee pensions, agricultural services, healthcare, education, skill development and employment, law enforcement, land reforms, elections and census" (NIMC, 2017).

This is a huge project, the scale and impact of which is not clearly defined in the published NIMC strategies, policies, frameworks and implementations. The underlying technical architecture of the Nigerian eID integration involves biometric data (fingerprints, iris scans and facial images), that is, sensitive personal data that raises a number of legal and ethical questions. In an ecosystem where there is no functional data protection law, and considering well-documented concerns related to emerging technologies (e.g AI, data and facial recognition) (Raji et al., 2020), many Nigerians have expressed deep concerns about the social desirability, effectiveness and cost of introducing and maintaining an eID system that is dependent on a central national database. Globally, one of the major concerns about national ID databases is related to the enormity of the power it bestows on the state. After the UK repealed its *Identity Card Act, 2006,* through the *Identity documents Act 2010,* the then Home Secretary Theresa May declared that: "This bill is the first step of many that this government is taking to reduce the control of the state over decent, law-abiding people and hand power back to them." This was a recognition that such a central database connected to almost all facets of life in the society changes the relationship between the individual and the state with high probability of encroaching on individual rights.

There are also critical questions of legal compliance and ethical responsibility related to potential impact on citizens' rights and values. This usually affects societal acceptance of such systems, which is why they are created after robust engagements with citizens. However, unlike similar projects that are undertaken in the global north, there is no documentation of any robust stakeholder impact assessment and engagement that could address potential ethical, legal, social and organisational challenges and concerns. There is also no empirical literature on citizens' concerns related to this technically, socially and culturally complex project. The question explored by this research is therefore: *what are the ethical, legal and socio-cultural impacts of the NIMC eID scheme that most concerns Nigerian citizens?* This paper is the first to provide insights into Nigerian citizens' concerns on the eID integration project. It is an exploratory study with these objectives: *to establish the ethical and legal implications of the current NIMC's electronic ID integration; to understand the citizens perception on the way these implications will have impact on their economic, political, social and cultural rights; and to provide recommendations to policy makers in order to ensure that risks are minimised while allowing the aims of the project to be met.* It starts with a historical account of national ID systems in Nigeria to the presentation of an empirical research that provides the citizens' perceptions of their fears and expectations of the eID integration. Through a mixed method approach, we present empirically grounded insights into the impacts of this innovation in Nigeria in light of the global drive towards digital ID for development.

2. Global electronic ID (eID) management system landscape

Digital identity can be viewed as a set of electronically captured and stored attributes which uniquely identifies an individual while a digital identification system uses digital technology throughout the identification life cycle which includes capture, validation, storage, transfer, identity authentication, verification, and credential management (Global Partnership for Financial Inclusion, 2018). We describe identity as a set of qualifiers and attributes which make an entity unique in the context of online or offline states while a management system is a digital framework which associates entities with their respective online and offline identities.

Due to the growing promise shown by digital identification, some countries have attempted to launch national initiatives to provide their citizens with digital identities (Pandya, 2019). Some countries already have foundational identification systems for the purpose of public and private sector administration and general identification such as national IDs (Gelb & Metz, 2018) whilst some have only functional identification systems which are used to manage the identity lifecycle of a particular service such as social programs, tax administration, and voting. In India, the national biometric identity system proposed by the Indian government called Aadhaar was accepted by the Indian Supreme Court but through a majority decision strict limits were placed on the application in other fields apart from financial, commercial and taxation purposes. The court rejected the application of the ID system in private phone systems, banking, and as an ID for students taking exams (Goel, 2018). In Turkey, the Turkish electronic ID card is based on the central registration system (MERNIS) and networked with other official databases such as the social security system, health and educational records and was introduced to the public in 2007 (Bozbeyoglu, 2011). In Peru, the National Registry of Identification and Civil Status (Registro Nacional de Identificación y Estado Civil, or RENIEC) is the national digital ID system and can be used as a form of identification for a wide range of public and private services. Pakistan's CNIC (Computerized National Identity Card), a core product of NADRA (National Database and Regulation Authority), is the legal digital ID card for Pakistani citizens. The SNIC can be used for both offline and online identification, voting, pension disbursement, social and financial inclusion programmes and other services. Other countries who have also implemented eIDs include Chile, Uruguay, Kazakhstan, Bangladesh, Mexico and some EU member countries.

The slow journey in the adoption of identity management systems has been hindered by a lot of challenges and rejection in some countries (Dahir & Mureithi, 2020; Dunn, 2020; Goel, 2018). In Kenya, it was ruled out because the country currently lacked a legislative framework to accommodate a biometric identity system and concerns about privacy and data protection. As mentioned earlier, the UK repealed its Identity Act owing to public concerns related to potential overreach of the government (Beynon-Davies, 2011). A national identity card system has also long been rejected in the United States (Krajewska, 2017). In Jamaica, the government claimed that the use of artificial intelligence and data science will create a new national identification system (NIDS) as a unique verifier of every citizen, using an enabling legislation approved by parliament in 2018 called the 'National Identification and Registration Act' (NIRA). The national ID system was deemed important to the country's economic development. However, the draft Act was met with stiff opposition due to the fact that it contained elements such as the highly intrusive level of biometric data being demanded, coupled with the compulsory nature of the plan, criminal sanctions for non-compliance, and the absence of adequate technical or legislative safeguards for data protection (Dunn, 2020). In 2019, the Jamaican Supreme Court rendered the act null and void and of no effect which was considered as a historic ruling in the country (Dunn, 2020). Other countries where mandatory national ID card enrolment has met strong opposition include Canada, Australia and Japan.

In developing countries, the need to migrate to an all-inclusive digital economy and to make the government and businesses more efficient is considered as one of the core factors for the adoption of digital identification (ID) initiatives. A good digital identification system unlocks good economic value and forms a method of inclusion for those who lack a digital identity. It also serves as an inclusion strategy for those who have a digital identity but cannot use it effectively in a digital cyberspace. As of 2019, of the 7.6 billion people on earth, 3.2 billion people have some form of digital ID and a digital trail, while 3.4 billion have some form of digital ID without a digital trail, and 1 billion people, particularly from less developed countries, appear to lack a legally

recognised ID (White et al., 2019). This shows that despite the benefits of digital identity management systems or electronic ID there is still a long way to go in unlocking the economic value accrued to individuals without a recognised ID and without a digital trail. Although several developing countries have implemented national eID systems, each with relative success, the slower adoption of eID in Nigeria is nuanced by the ethical, legal and socio-cultural concerns of Nigerian citizens.

Whitley and Hosein (2010) in their book reviewed a range of national identity policies and documented the global challenges facing these policies. A persistent argument in the debate surrounding the adoption of a mandatory national eID system is the possibility of leading to a "big brother" state. There is also the consideration of the lack of adequate data protection laws or lack of an appropriate legislative framework in many of these countries and the potential violation of citizens' right to privacy. Jean-Jacques Rousseau in his book *The Social Contract,* declared that "Man is born free, and he is everywhere in chains". In describing the surveillance powers that can be bestowed on the state by such electronic databases, Haggerty and Ericson (2000) adapted this to "Humans are born free and are immediately electronically monitored". This is a reminder of the potential surveillance issues associated with national electronic ID databases and the need to preserve citizens' rights to privacy. In many instances, the use of identity management systems can on one hand define the rights to citizenship and on the other hand enable irresponsible surveillance of citizens (Bozbeyoglu, 2011).

It is clear that despite opposition to mandatory national ID card system in many countries due to identifiable concerns, a number of countries have established eID management systems[1] either as centralised or decentralised infrastructures. Whereas both approaches have their shortcomings in different contexts, many of the established eID management systems with higher reported cases of abuse and concerns are characterised by their centralised approaches and include systems developed in India and Uganda. The decentralised systems implemented such as the e-Estonia for instance, receive less criticism because citizens have clear control over the use of their ID and data, which is considered by many as the ultimate or logical endpoint for identity systems worldwide (Hersey, 2021). India's Aadhaar system looks the closest to NIMC's eID system in that it is an all-encompassing ID system built on a centralised approach. This is a system that has received criticism from a number of international institutions including Privacy international[2] and Access Now[3] This means that similar concerns might be raised for the Nigerian system.

3. National eID management system in Nigeria

The project to establish an effective National ID management system in Nigeria has had a checkered history to say the least. So far, the history of Nigeria's National ID schemes has been fraught with allegations of corruption, infrastructural and privacy concerns, low levels of public awareness and socio-cultural constraints. It has a history characterized by questionable contracts with local and foreign companies including major players like Chams PLC (Okonji, 2019), Sagem (Ibekwe, 2015) and Mastercard (Court, 2014). Indeed, Nigeria's framework to establish a national ID system was first conceptualized in 1978 when the Department of National Civil Registration (DNCR) was first established by the Federal Ministry of Interior. Between 1981 and 2001, Nigeria signed a number of contracts with private partners (such as Avant Incorporated and Chams plc) to create National ID cards at the cost of billions of Naira. All of these initiatives failed because of what (Ibekwe, 2015) described as "executive high-handedness, mind-boggling corruption, sheer irresponsibility of government officials and asinine abuse of power''. In 2001, another private firm, Sagem (A French Tech Company partly owned by the French government) was given a contract to produce 70 million ID cards (Michaels, 2004). After five years of national data collection, Sagem produced about 37 million National ID cards. The project was discontinued and a number of government officials were implicated in a bribery scandal and Sagem was subsequently fined by a French court for having paid bribes to secure contracts in Nigeria.[4] The system and the data collected were never reused, and to date, the status of the personal data collected by Sagem remains unclear as there is no evidence of the destruction of the created database. Following the Sagem scandal, the NIMC Act was passed into law in 2007 establishing the National Identity Management Commission (NIMC). Since then, the NIMC has partnered with MasterCard, Visa, Verve, the National Communication Commission (NCC), the Central Bank of Nigeria (CBN), local banks, network operators, intelligence agencies and other government and private agencies to ensure the creation of an integrated ID ecosystem. In 2013, the NIMC announced a partnership with MasterCard to produce the eID cards with electronic payment capability as a pilot program – a multipurpose card that was supposed to serve as a driver's licence among other things (Osuagwu, 2013). In 2014, MasterCard issued the first eID cards at an official launch where President Goodluck Jonathan received his MasterCard-branded eID card[5]. However, following the award of the contract to MasterCard, the company was accused of using dishonest means to side-line local companies - Chams PLC and Chams Consortium Ltd to win the project (SaharaReporters, 2019). A legal action was subsequently instituted against MasterCard. This case informed the decision of a Nigerian court in 2019 that ordered MasterCard and the 22 Nigerian banks working with them to stop the production and issuance of the national eID produced by MasterCard (Ogunfuwa, 2019).

The current NIMC effort supported by the World Bank and termed *Digital Identification for Development (ID4D)* is an attempt to focus on digital integration of the different ID systems. Conceived in collaboration between the World Bank, the Agence Française de Development (AFD), and European Investment Bank (EIB), Nigeria's ID4D is aimed at achieving strategic objectives for universal ID and civil registration systems implementing best practices (World Bank, 2019). It is hoped that this project will close the gender gap in ID access, and foster inclusion for marginalised groups by strengthening the legal and institutional framework, establishing a robust and inclusive foundational ID System, enabling access to services through IDs and stakeholders' engagement. However, how the current implementation of this project is fulfilling these objectives as well as preserving the fundamental rights of the citizens (including privacy rights) is yet to be determined. With the Nigerian data protection bill yet to be passed into law, the ethical and legal implications of processing and storing highly sensitive data of citizens in a centralised database are not yet fully assessed.

Although, many citizens' data are already collected and stored by a number of agencies including Nigeria Population Commission (NPopC), National Health Insurance Scheme (NHIS), Federal Inland Revenue Service (FIRS), Joint Tax Board (customs), National Social Safety Net Project (NASSP), Federal Ministry of Agriculture and Rural Development (FMARD), National Pensions Commission (PENCOM), Independent National Electoral Commission (INEC), security agencies such as; Ministry of defence (MoD), National Immigration Service (NIS), Federal Road Safety Corps (FRSC), Nigeria Prison Service, Nigeria Police Force (NPF), state and local agencies, and actors from the private sector (Financial institutions, Telecom service providers and Healthcare

[1] https://www.worldprivacyforum.org/2021/10/national-ids-and-biometrics/

[2] https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar

[3] https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf

[4] https://www.bbc.co.uk/news/business-19498916

[5] https://foreignpolicy.com/2014/09/03/nigerias-orwellian-biometric-id-is-brought-to-you-by-mastercard/

service providers). The new system involves compulsory registration at designated collection points. At the completion of enrolment into the National Identity Database (NIDB), a National Identification Number (NIN) is assigned to legal residents in Nigeria (citizens and non-citizens). The NIN is tied to all records about an individual in the database and is also used to establish or verify his/her identity. Subsequently, a national eID card will be issued to Nigerian citizens with a valid NIN which can be used currently for Europay, MasterCard, and Visa (EMV) payment, verification, security, e-SIM application, and travel. There are also proposals to expand its usage to what is called 'applets' including for e-Health, e-Pension, e-Voting, e-Taxation, e-Drivers' License application, e-Transport, e-Insurance application. Almost all aspects of a Nigerian citizens' life will be tied to this eID built on a central database of highly sensitive personal data and under the control of the Federal government. Whereas this is a laudable initiative, the complex technical infrastructure, cost, big data and implementation demand has raised ethical, legal, economic and socio-cultural concerns that require more consideration.

In August, 2020 the NIMC made the Android and iOS versions of its Mobile ID app capable of generating the digital National Identification Number (NIN) of a successfully enrolled citizen available on Google Playstore and Apple store. This proved to be an insecure application that incorrectly generated personal information of random citizens raising concerns that bothered on privacy and security. Following these concerns, the NIMC pulled the app from Playstore and iOS store two days later, putting out a statement that this was a ''novel innovation…yet to be officially approved for public consumption'' (Adesanya, 2020). This illustrates that the current process lacks high-level impact assessment of the technology which puts citizens at profound privacy and security risks, including human rights risks.

In 2009, a "Privacy Impact Assessment" (PIA) was conducted on the then National Identity Management System (NIMS) strategy.[6] This PIA identified a number of potential legal, ethical, technical and cultural concerns and made recommendations for ensuring the security of personal data. However, a lot of changes have happened since then, Nigeria has a new administration and the technical focus of the eID system changed substantially, as new technologies are being implemented by new actors. Did the NIMC conduct a stakeholder impact analysis or a data protection/privacy impact assessment on the new data processing systems in light of these developments? If this was done, what is the evidence that any identified concerns were adequately mitigated? These are questions to which answers are not readily available for the Nigerian public and all stakeholders involved. Nigeria is yet to have a functional data protection legislation, which means that privacy and security issues remain major concerns as the implementation of the digital identification processing biometrics continues.

4. Nigerian data protection ecosystem

For a long time, the Nigerian data protection ecosystem was largely unregulated and fragmented with the constitution providing a broad right to privacy but not specifically, the right to data protection.[7] Nonetheless, there were sector-specific laws[8] creating data protection obligations enacted by the legislature or issued by sector-specific regulators.[9] However, the approach was limiting and failed to protect the human rights of consumers. In addition, the laws were largely unenforced and there was a lack of clarity concerning the role of the regulators. Albeit, there have been different legislative attempts at enacting a law with little success. The most recent effort is the Nigeria Data Protection Bill 2020 and another significant effort is the Digital Rights and Freedom Bill 2019 that is currently awaiting the House of Representatives Committee Report.

In 2019, the National Information Technology Development Agency (NITDA) released the Nigeria Data Protection Regulation (NDPR), which represented the most comprehensive effort to regulate the protection of personal data. The NDPR introduced Data Protection and the importance of compliance to principles of privacy to the social consciousness The Regulation created obligations on data controllers and processors and rights for data subjects. It also stipulated principles that the data processing entities were required to adhere to. Any breach of those principles resulted in prosecution. This regulation applies to both private and public organisations. One of the obligations on controllers and processors is the guarantee of security of personal data.[10] This is further reinforced under Section 28 of the National Identity Management Commission Act, which criminalises unlawful access to identity databases. The NDPR designated NITDA as the regulator to enforce the regulation. The NDPR's is supported with a Data Protection Implementation Framework (DPIF), which was released in November 2020. The framework complements the NDPR to;

> "ensure a tailored implementation of Nigeria's data protection regime. In addition, it serves as a guide to data controllers and processors to understand their respective compliance obligations."[11]

However, in 2022, the establishment of a new agency, the Nigerian Data Protection Bureau (NDPB), was approved. NDPB is expected to take over enforcement of compliance with the provisions of the Nigeria Data Protection Regulations 2019 (NDPR) from NITDA.

The right to privacy has been recognised by the court in the case of *EMTS v Godfrey Eneye*.[12] Right to data protection has also been recognised by the court as a subset of the right to privacy guaranteed under Section 37 of the Nigerian Constitution and demonstrated in the case of *Digital Right Lawyers Initiative v NIMC*.[13]

As regards NIMC's national identity program, the issue of privacy and data protection has been a recurrent theme between the National Identity Management Commission (NIMC) and civil society groups. The contention has been focused on the propriety of a national electronic identity program in the absence of a comprehensive data protection law. The lack of a comprehensive law cannot guarantee sufficient safeguards to protect the rights of individuals. In 2015, Paradigm Initiative sued the NIMC for entering a contractual arrangement with MasterCard to provide electronic identity (Onalaja, 2015). In 2019, the organisation called on the NIMC to suspend the mandatory enrolment for the National Identity Program until there is a comprehensive data protection law (Paradigm Initiative, 2019). An advocacy group has also sued to ask the court to stop the NIMC from processing data on its mobile application pending when reported privacy concerns have been resolved (Ifeoma, 2020). Although the NIMC has denounced reported cases of possible cyber-attacks on the national database (Elebeke, 2020), the possibilities of such attacks remain.

5. Methodology

The full-scale study carried out here was done with a questionnaire designed to collect quantitative data which was based on the findings of a pilot study that was qualitative. This can be described as an *exploratory*

[6] https://nimc.gov.ng/docs/pia_report.pdf

[7] Section 37 of the Nigerian 1999 Constitution

[8] Examples include the Credit Reporting Act, Child Rights Act, Freedom of Information Act, National Identity Management Commission Act, National Health Act, and Cybercrimes (Prevention and Prohibition) Act

[9] Some Regulations, Guidelines, Framework have been released by regulators. Examples are the National Identity Management Commission, Central Bank of Nigeria, Nigeria Communication Commission, and National Information Technology Development Agency.

[10] Article 2.6 NDPR

[11] https://techhiveadvisory.org.ng/wp-content/uploads/2021/09/Africa-ReportFoEDP.pdf

[12] (2018) LPELR-46193(CA)

[13] Unreported Appeal No.: CA/IB/291/2020

sequential mixed method approach because the study began with a qualitative phase and moved sequentially to a quantitative phase. As Creswell and Clark (2017) pointed out, exploratory sequential mixed method approach describes a method of combining qualitative and quantitative methods in a sequence of phases. The underlying rationale for this approach lies in an attempt to explore reality before making decisions on what variables need to be measured. The qualitative results are often used to create conceptual themes or elements that can be studied in the quantitative phase (Curry & Nunez-Smith, 2014). The outcomes of the qualitative phase are thus integrated into the design of the quantitative approach in a process called *building* (Onwuegbuzie et al., 2010). The quantitative phase is traditionally used to verify, confirm, or generalize the initial exploratory qualitative findings (Clark & Ivankova, 2015). The qualitative phase of this project, which can best be described as a pilot study, used a questionnaire designed to collect qualitative data to identify possible citizens' concerns related to the eID integration. The results of this qualitative phase subsequently shaped the design and scope of a quantitative phase used to understand what Nigerians are most concerned about. The research received Ethics approval from the De Montfort University's Ethics approval committee and considered and mitigated identifiable concerns related to participants' informed consent, privacy and confidentiality.

5.1. Research design

5.1.1. Qualitative phase

The questionnaire was designed for only experts who are well informed on the technical infrastructure and its implementation, and can identify potential impacts on the citizens. These include Nigerian legal, data ethics, policy and technology experts. The questionnaire asks participants to identify the legal, ethical, cultural, social and economic impact of the NIMC eID integration program. This was disseminated online to purposively sampled participants with relevant expertise. The questionnaire was sent to 38 participants and 20 participants in total responded to this questionnaire (*see Table 1*). These experts were drawn from civil society groups and Universities in Nigeria. These were people identified to be working in policy related initiatives or teaching public policy related courses at the University level. To avoid conflict of interest, experts from industry were excluded because many companies are now collaborating with NIMC on the project.The intention was to gather the constructive interpretation of these experts' understanding of the possible impacts of the eID integration citizens can or should be worried about. Their answers were thematically analysed and a number of concerns emerged as follows: *possibility of data theft, irresponsible data sharing, privacy and security of data, lack of effective data protection regulation, lack of informed consent, possibility of increased government surveillance, misuse of data for discrimination/exclusion, misuse of data for commercialization, possibility of human rights abuses* and *concerns related to the role of international tech companies in the process.* These results formed the integral part of the quantitative phase.

5.1.2. Quantitative phase

Following the findings of the qualitative phase, a questionnaire was designed to collect quantitative data from Nigerian citizens who were the target population. The fundamental difference between the initial questionnaire and the subsequent questionnaire is that each was designed to get different types of data. The qualitative questionnaire aimed at collecting expert interpretations of participants regarding the possible concerns related to the eID integration program. Therefore, the reality was socially constructed by social actors while this questionnaire focused on the objective measurement or statistical analysis of the identified reality. The data collected during this quantitative phase were thus analysed via a descriptive statistical analysis method (using textual and visual representations). The statistics provide a description of how the citizens view the implications of the eID integration in Nigeria. Thus, participants were asked to indicate which of the identified possible concerns are the most worried about. The questionnaire was disseminated virtually via different platforms: WhatsApp, Facebook, LinkedIn, Twitter and Instagram. Online questionnaire was chosen because according to the global data platform *Statista*, as of July 2021, there were more than 108 million internet users in Nigeria. In August 2021, 48.12% (over 101.7 million) of the Nigerian population was reported to be using a mobile device to access the internet (Johnson, 2021). Among these internet users (who are aged between 16 and 64), these social media platforms were among the most used internet platforms with whatsApp popular with 93% of the users, Facebook 86.2%, Instagram 73.19%, twitter 61.4% and LinkedIn 32% (Sasu, 2022). This is more than half of the population the NIMC eID scheme is also targeting. 305 participants responded and the results are presented below. 52.8% (161) of these participants were male while 47.2% (144) were female. There was also a good mixture of citizens who were non-graduates (30.8% - 94), graduates (32.5% - 99) and postgraduates (36.7% - 112), providing diversity of opinions across the board. 89.8% (274) of participants indicated that they have enrolled in the National ID database while 10.2% (31) have not.

Table 1
Distribution of the research participants for the qualitative questionnaire.

Participants' expertise	Number of participants
Policy	6
Data Ethics	6
Technology	4
Legal	4

6. Results

For the participants who have not enrolled, their reasons ranged from the cost attached to it (about N5000 naira registration fee), lack of registration centres where they lived, "not gotten round to it" to concerns related to continued collection of citizens personal data for multiple reasons by the government. The participants who indicated that they have enrolled were then asked whether they trust the government to use their data responsibly. 66.4% (182) indicated that they do not trust the government while 33.6% (92) do trust the government (*see Fig. 1*). This is a significant percentage of the population who do not trust the government with their personal data. Whereas the underlying factors behind this lack of trust deserves deeper exploration, these participants (those that do not trust the government with their data and those who have concerns regarding registration) were asked to indicate which of the identified concerns worried them the most *(see Fig. 2)*.

7. Critical discussion and possible consideration of responsibility by design principles

Considering the current global data-driven ecosystems, characterised by sophisticated data breaches (Hammouchi, 2019), it was no surprise that Nigerians identified privacy and security of data as the most critical concern. Advancements in technology, particularly Artificial intelligence (AI), deep learning and machine learning introduce new threats to data privacy and security. The implementation of the NIMC's integration program relies on a centralised data management system that stores and manages access and application of the personally identifiable information of users with an albeit multi-layered approach that includes encryption. However, just like the debate that emerged, particularly in Europe as the COVID-19 pandemic's contact tracing tools were being developed, encryption is an insufficient privacy-preserving technique in a centralised database. Following an analysis of the developed digital contact tracing protocols in Europe, Vaudenay, (2020) concluded that a centralised national database puts the anonymity of all users in high danger, especially against a malicious authority or individual actors. It

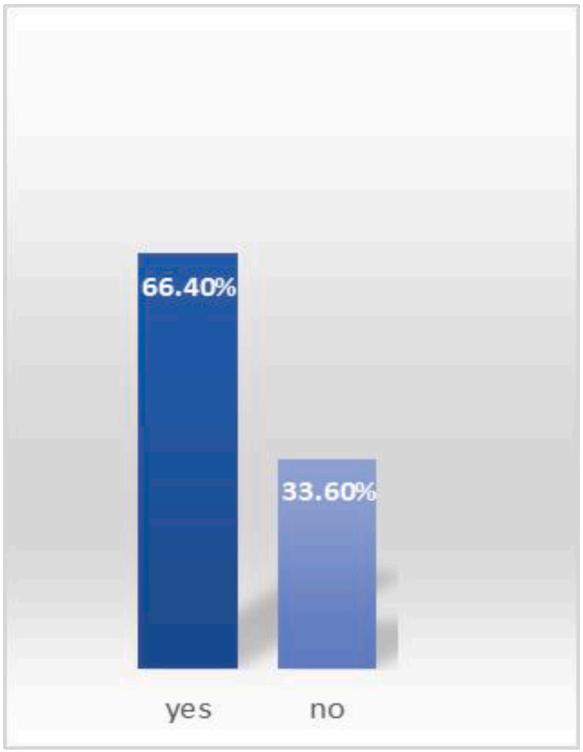

Fig. 1. Trust in the Nigerian government with data provided for the NIMC eID management system identity program. The majority of the participants ranked privacy and security of data (75.6%) as their most critical concern, followed by possibility of human right abuses (54.9%). Possibility of misuse of data for discrimination/exclusion (54.5%) ranked third on the list of concerns citizens are worried about and lack of effective data protection regulation (53.1%) in Nigeria was the next. Other concerns are ranked in this order: possibility of irresponsible data sharing by government officials (49.3%), possibility of data theft (47.4%), possibility of increased state surveillance (44.6%), possible commercialization of the data (41.8%), lack of informed consent observed in the current process (38.5%) and concerns related to the role of international tech companies involved in the process (25.8%). These results reveal a pattern of the concerns which are not dissimilar to concerns related to eID integration initiatives in other countries of the world but the contextualization of these findings in Nigeria is very crucial to their understanding.

enables security attacks and increases the possibility of data theft at a larger scale than in a decentralised system. A malevolent actor or authority can compromise the privacy and confidentiality of all users if the security of the central server is breached. Biometric data (finger prints, iris scans, face) are highly sensitive data that are easily re-identifiable. Privacy and security concerns related to this are therefore valid.

The possibility of human right abuses aligns well with the strongest argument against national ID cards in the UK which is that it would fundamentally change the relationship between citizens and state actors. For the most vulnerable people in society, this NIMC eID program will be life-changing. If one is unable to enrol or if the biometric authentication doesn't work, people could be denied state benefits including pension or be unable to access credit facilities and insurance. What considerations have been given to old and frail citizens whose fingerprints have faded or citizens with genetic mutations such as *adermatoglyphia* (Stromberg, 2014) that do not have functional fingerprints? What of citizens too ill to go through the new bureaucratic process to enrol? Many citizens including people with valid reasons not to trust the Nigerian government with their personal information stand the chances of losing some of their fundamental rights or being excluded.

Additionally, such a big national database with over 100 million Nigerians that can facilitate a complex data processing ecosystem without a robust data protection law is very concerning. Data protection laws are critically important because they provide guidance and best practice rules for both private and public organisations to follow in processing personal data and to protect the rights of the data subject. With the possibility of using these data to train AI systems, data subjects are exposed to increased risks and thus require protection. Given that the history of digital ID in Nigeria has been mired in corruption as was observed earlier in Section 3 and reported extortions at enrolment centres[14], possible irresponsible sharing of citizens' data by government officials is a valid concern. This concern is further justified by the big misstep that led to the leakage of some Nigerians' personal data via NIMC app in 2020. This is also closely related to the data commercialization concerns. As Nigeria's data demands grow, so too the opportunities for those investing in the market's infrastructure. The idea of commercialising citizens' data in any shape or form raises ethical and legal questions bothering on public trust and expectations, consent and balancing the interests of private actors and citizens' rights. Such commercialization can also lead to data breaches as was the case in India where a reporter from a national Newspaper tried and succeeded in buying the data of 1billion Indians for less than £10 (Khaira, 2018).

It is evident that there is also a good section of the population that do not trust the government which may be tied to possibilities of utilising the system for r purposes unrelated to genuine public interests including possibility of increased government surveillance, human rights abuses and misuse for commercialisation as indicated by the results. Whereas the underlying intentions of giving people proof of identity and providing economic and social benefits are good, a public malicious authority can also misuse the data; for instance, for increased surveillance of the citizens. Such a centralised database puts too much power in the hands of the government to become overly intrusive. The control over citizens increases with a central national database linked to all facets of life, controlled and managed only by the government. Citizens can arbitrarily be prevented from voting, getting insurance or travelling around the country for reasons only a malicious government can decide. There is a real risk that the eID scheme can aid institutional discrimination and state surveillance. In India, the impact of the national ID system has been similarly described as 'exclusion by design' because of inaccessibility of social protection by vulnerable people (Privacy International, 2021). In Uganda, a study of the impact of the Ugandan national identity card system (also known as 'Ndaga Muntu') reported that the system is a 'cocktail of discrimination'(Unwanted Witness, 2020). As Fadesere (2018) has observed, the Nigerian government has failed to secure the commitment of its citizens in policy implementation in the last decade which has led to lack of trust in the government. It is from this mistrust that the concern related to social exclusion and discrimination emerge from.

Furthermore, the NIMC enrolment program allows the provision of personal data without informed consent. This means that citizens are mandated to provide their information to the government without receiving sufficient information about the processing, full comprehension of the dynamics of the processing and do not exercise the voluntariness expected of a human person. Citizens are not provided precise information on who will have rights to access their data and for what reason. This simply undermines public trust and confidence in the scheme. The final concern relates to the unclear roles of international companies involved in the process. Despite the bribery scandal involving Sagem in a contract worth about $214m, the NIMC surprisingly retained the services of IDEMIA to provide the automated biometric identification system and maintenance support for NIMC's ID database. After series of name changes in the last two decades (e.g, Sagem Défense Sécurité, Sagem Orga, Safran, OT-Morpho) IDEMIA represents the interests of the same company (Sagem) fined in France for bribery and

[14] https://www.thecable.ng/nimc-vows-to-clamp-down-on-extortion-during-nin-enrolment-after-thecables-report

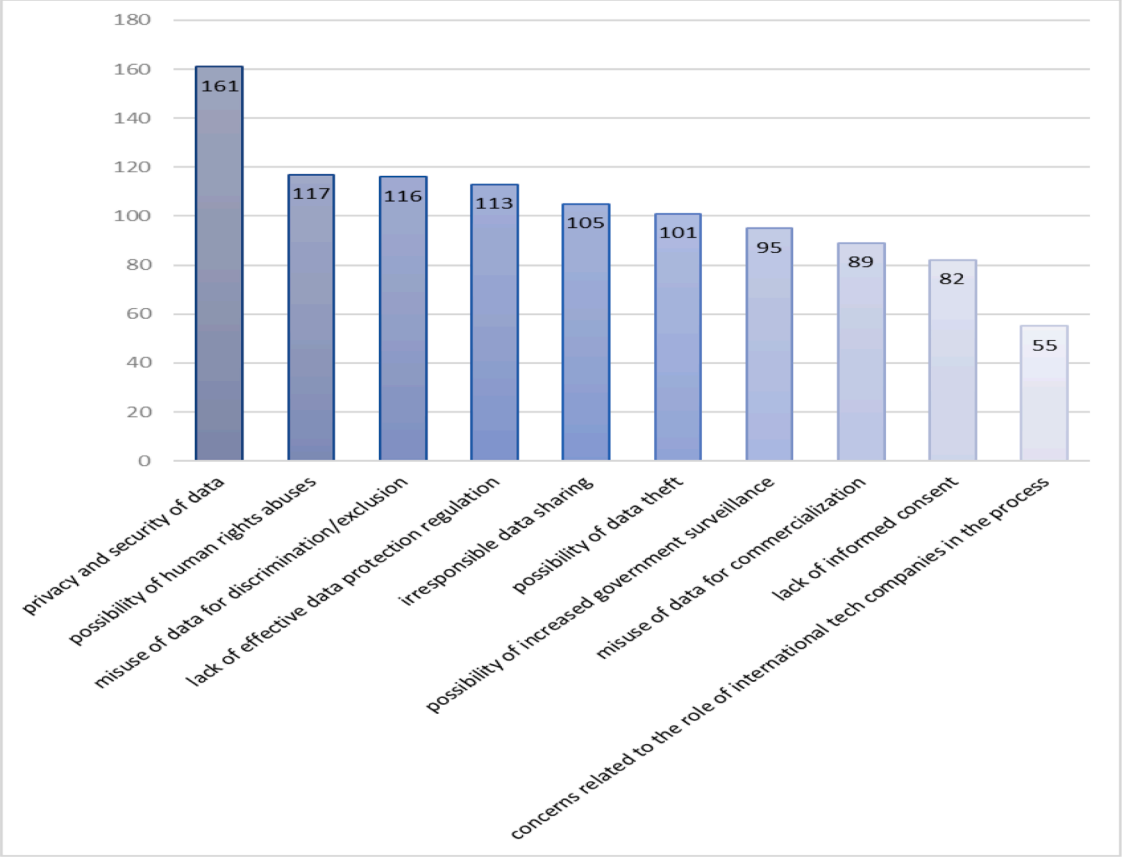

Fig. 2. Ethical, legal and socio-cultural *concerns Nigerians are most worried about.*

corruption in Nigeria. Announcing the deal on their website on the 4th of April, 2017, the company called this a "renewed service and maintenance contract". Is this basically the renewal of the contract at the centre of the corruption scandal? This is a question Nigerians and all relevant stakeholders deserve an answer to. The continued involvement of this company in the processing of Nigerian' personal data is very ambiguous and should be a source of ethical and legal concern for all Nigerians.

Whereas the proposed benefits of the NIMC integration is undebatable, the design and implementation of such a system that will fundamentally shape the socio-cultural, economic and political life of the society should consider the above concerns. There is clear evidence that a robust consideration of the potential impacts of this technological innovation was lacking in the design and implementation. To be a transparent, fair, inclusive, responsible and sustainable innovation, the government should consider an approach that sufficiently considers citizens' concerns, fears, hopes and expectations. This is a system that should aim not only to be legally compliant, but ethically responsible and socially acceptable. The approach that comes to mind here, considering the ethical, legal and socio-cultural impacts of the NIMC eID integration, is the Responsible Research and Innovation (RRI) or Responsibility-by-Design (RbD) approach. To mitigate these identifiable concerns, RbD can provide an effective approach of embedding values such as privacy, inclusion, justice, fairness and trust into the technical design of the system. RRI, which has become an important research and innovation approach for the design and deployment of technologies, particularly in Europe is a "transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)'' (Von Schomberg, 2012). It is meta-responsibility that shapes innovation processes with a view to ensuring desirable and acceptable outcomes (Stahl, 2013). RRI provides a framework for technology assessment in a way to embed normative values into the design and implementation of the technology. Exploring this approach or framework with its anticipatory (anticipating and analysing the impacts or consequences of the technology), reflexive (reflecting on the purposes of and motivations for the technology), inclusive (engaging with relevant stakeholders where necessary) and actionable (developing actions that influence the direction of the innovation) elements is something the NIMC eID integration needs for better and responsible outcomes.

8. Recommendations

The full technical process involved with innovation must be fully transparent. The protocols and their implementations including all components provided and managed by local and international companies must be available for public analysis. The role of each individual private sector actor involved in the process should be well defined. Preventing companies of questionable repute from working with collected data can go a long way in building public trust in the system. This can start with clarifying the involvement of IDEMIA in this process. How the data is collected, stored and who should have access to the data and for what must be documented unambiguously. More improved transparency from the government will help to ensure a better-informed public debate on the prospects and challenges of the system.

There is an urgent need for increased citizens' participation in the process through robust stakeholder engagements. Nigerian citizens, industries and civil society groups need to be engaged to fully understand the potential impact of this innovation and how to respond to them. Deliberative democratic approaches such as citizens' juries, citizens' assemblies, public dialogues, workshops, polls, and stakeholder consultation tools can be used to shape empirically sound decisions

related to this integration scheme. Being open to such engagement initiatives that could inform future iterations of the eID system will provide better outcomes for the society at large. The rights of individuals rather than institutions should be prioritised in the process.

There are scientific, legal and ethical arguments to suggest that a decentralised data management approach will be more privacy preserving in this context. It reduces the chances of a large-scale data breach/or data theft. Decentralised data management systems have been found to be more likely to comply with both human rights and data protection regulations and the rights of every Nigerian citizen should be the priority of policy makers. It also enhances trust in the system. However, if the use of the centralised approach continues, there is a need to make available the result of any risk assessment conducted on the eID system and the mitigation approaches adopted to address citizens' concerns, particularly, the most vulnerable in the society. The government should provide guarantees in the form of legal safeguards for citizens that the data collected will not be used to discriminate against them, will not be used for dual use of concern (e.g for unacceptable military application) and will not be used for intrusive surveillance of citizens. Since the eID system is a malleable technology characterised by unintended consequences, such a legal safeguard is necessary to protect citizens from identified and unidentified risks. This should then be accompanied by a clear and targeted awareness program focused on communities to build trust and confidence in the process. These are important to ensure that the fundamental human rights are protected against malicious state and private actors as well as from automated decisions. Our findings demonstrate that the Nigerian eID management system did not pay close attention to the well articulated principles on identification for sustainable development by the World Bank Group (2021). For a socially acceptable, ethically responsible and legally compliant eID system in Nigeria, the 10 principles under the three pillars of inclusion, design and governance need to be adhered to.

9. Limitations of the study and future research

These research outcomes are critically important for the continued development and implementation of the eID harmonisation and integration system. A mixed method approach provided an opportunity to gain both interpretive and positivist insights from participants but understanding citizens' concerns requires more interpretive insights that this research did not provide which can be perceived as a limitation. The sample size of the qualitative phase of the study can be considered too small to provide a holistic citizens' perspective on the ethical, legal and socio-cultural impacts of the national eID system. Further research can involve more qualitative research that can provide more insights into the social interpretations (e.g through Focus Groups, interviews and ethnography) of the concerns not only by experts but by citizens.

Additionally, since the target population for this study was the over 100 million Nigerians eligible for the eID enrolment, the sample size of 305 in the quantitative phase may be perceived by some as not fully representative of the population. However, the fair gender and educational status distribution of the participants introduces sufficient elements in the sample that can improve external validity or generalizability of the findings. What is missing is the potential differences in the understanding of these concerns based on citizens' economic status, ethnic background, religious beliefs or political affiliations. The exploration of the complex relationships between these variables and the identified concerns with a larger sample size should be a theme for further research. It will also be insightful to analyse these concerns with technology acceptance and adoption theories (Taherdoost, 2018) such as Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), Theory of Interpersonal Behaviour (TIB), Igbaria's Model (IM), Social Cognitive Theory (SCT), Diffusion Innovations Theory (DOI), Perceived Characteristics of Innovating Theory (PCIT), Motivational Model (MM) or the Unified Theory of Acceptance and Use of Technology (UTAUT). Although some of these theories emerge from established disciplines such as Sociology and psychology, they offer reasoned insights into social acceptance or rejection of novel technologies. A Responsibility-by-design analysis of the system (NIMC eID scheme) would also provide good insights into the practical approaches that can help in embedding values into the design and implementation of the system.

10. Conclusion

In this paper, we have highlighted the critical ethical, legal and socio-cultural concerns related to the centralised storage, management and application of citizens' biometrics in the NIMC eID scheme and identified which of these concerns the citizens are most worried about. It has revealed that the lack of transparency associated with the mandatory collection of citizens' unique and distinctive characteristics of the use of biometric technologies and the possibility of applying AI algorithms on these data raise concrete risks. The paper suggests that the application of such a national database could enable breach of fundamental human rights including unreasonable surveillance of citizens for reasons that can be defined only by the government if there are no legal remedies that can protect the citizens. It then suggests that the government should not only consider specific legal safeguards for citizens in this regard, there should also be consideration of other technical alternatives that are more privacy-preserving, fair, equitable, trustworthy and inclusive. The continued implementation of the centralised approach requires a more robust risk assessment to address existing and emerging risks to the rights, ethics, and freedoms of all citizens.

This paper makes contributions to the ongoing discourse on technology for and with society. It is a pointer to the importance of including the visions, expectations and fears of the society in innovation to achieve social acceptability, legal compliance and ethical responsibility. The logical malleability of technology results in many unintended consequences for the society or for a particular group of people and these require reasoned reflections, public engagement and responsive actions in both the design and implementation stages. The eID management system as a social innovation demands responsibility-by-design approaches that consider unique Nigerian values, principles, local contexts and interests and that can ensure that broader societal concerns, as identified in this paper, are sufficiently addressed. The eID system is a technology that is not value neutral, rather it is value-laden: it can influence actions and it can also change socio-cultural dynamics. Mitigating its possible risks, concerns and challenges should become a priority not only for policy makers but also for people who are developing it. There is a need to understand better the power dynamics at play with the eID system and the dependencies it creates.

Funding

DE, SA and PO were supported by the European Union's Horizon 2020 Framework Programme for Research and Innovation under the Specific Grant Agreements No. 945539 (HBP SGA3).

CRediT authorship contribution statement

Damian Eke: Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Ridwan Oloyede:** Writing – original draft, Writing – review & editing. **Paschal Ochang:** Writing – original draft, Writing – review & editing. **Favour Borokini:** Writing – review & editing. **Mercy Adeyeye:** Writing – review & editing. **Lebura Sorbarikor:** Writing – review & editing. **Bamidele Wale-Oshinowo:** Writing – review & editing. **Simisola Akintoye:** Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial

interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Adesanya, A. (2020). National identity app not yet approved for public use—NIMC. *Business Post*. https://businesspost.ng/general/national-identity-app-not-yet-approved-for-public-use-nimc/.

Beynon-Davies, P. (2011). The UK national identity card. *Journal of Information Technology Teaching Cases, 1*(1), 12–21. https://doi.org/10.1057/jittc.2011.3

Bozbeyoglu, A. C. (2011). Citizenship rights in a surveillance society: The case of the electronic ID card in Turkey. *Surveillance & Society, 9*(1/2), 64–79.

Clark, V. L. P., & Ivankova, N. V. (2015). *Mixed methods research: A guide to the field (Vol. 3)*. Sage publications.

Court, A. (2014). Branding Nigeria: MasterCard-backed I.D. is also a debit card and a passport. Cnn.Com. http://edition.cnn.com/2014/09/25/business/branding-nigeria-mastercard-backed-i-d-/index.html.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.

Curry, L., & Nunez-Smith, M. (2014). *Mixed methods in health sciences research: A practical primer (Vol. 1)*. Sage publications.

Dahir, A., & Mureithi, C. (2020). *Kenya's High Court delays national biometric ID Program*. New York Times. https://www.nytimes.com/2020/01/31/world/africa/kenya-biometric-ID-registry.html.

Dunn, H. S. (2020). Risking identity: A case study of Jamaica's short-lived national ID system. *Journal of Information, Communication and Ethics in Society*.

Elebeke, E. (2020). *NIMC debunks claim on breach of database*. Vanguard Newspapers. https://www.vanguardngr.com/2020/12/nimc-debunks-claim-on-breach-of-database/.

Fadesere, T. (2018) Nigerians do not trust Government. Stears Business.

Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution. Center for Global Development Working Paper, 315.

Gelb, A., & Metz, A. D. (2018). *Identification revolution: Can digital ID be harnessed for development?* Brookings Institution Press.

Global Partnership for Financial Inclusion. (2018). *G20 digital identity onboarding*. World Bank. https://books.google.co.uk/books?id=TZc8zQEACAAJ.

Goel, V. (2018). *India's top court limits sweep of biometric ID program*. The New York Times. https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622.

Hersey, | Frank (2021) Centralized, decentralized or neither: Which national digital ID system will you choose? | Biometric update. Available from: https://www.biometricupdate.com/202112/centralized-decentralized-or-neither-which-national-digital-id-system-will-you-choose [Accessed 24/03/22].

Hammouchi, H., et al. (2019). Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time. *Procedia Computer Science, 151*, 1004–1009.

Ibekwe, N. (2015). *Over N121 billion wasted, Nigeria's troubled National ID Card project in fresh controversy*. Premium Times. https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html.

Ifeoma, P. (2020). National digital identity card: NGO seeks injunction against NIMC over data breach…. DNL legal and style. https://dnllegalandstyle.com/2020/national-digital-identity-card-ngo-seeks-injunction-against-nimc-over-data-breach/.

Johnson, J. (2021) Nigeria internet user penetration 2026. [Online] Statista. Available from: https://www.statista.com/statistics/484918/internet-user-reach-nigeria/ [Accessed 25/03/22].

Khaira, R. (2018). *Rs 500, 10 minutes, and you have access to billion Aadhaar details*. The Tribune. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

Krajewska, M. (2017). *Documenting Americans: A political history of national ID card proposals in the United States*. Cambridge University Press.

Lyon, D. (2009). National IDs in a global world: Surveillance, security, and citizenship. *Case Western Reserve Journal of International Law, 42*, 607.

Michaels, D. (2004). An odd couple gets hitched. *The Wall Street Journal*. https://www.wsj.com/articles/SB109902974933559595.

National Identity Management Commission Act. (2007). *National policy and institutional framework for an identity management system for Nigeria* (2005). National Identity Management System https://www.nimc.gov.ng/docs/reports/nimc_act.pdfNIMC (2005).

NIMC. (2017). *A strategic roadmap for developing digital identification in Nigeria*. National Identity Management System.

Ogunfuwa, I. (2019). *Court stops production of ID cards by Mastercard*. Punch Newspapers. https://punchng.com/court-stops-production-of-id-cards-by-mastercard/.

Okonji, E. (2019). *Court restrains Mastercard from issuing national identity cards*. ThisDay Live. https://www.thisdaylive.com/index.php/2019/11/19/court-restrains-mastercard-from-issuing-national-identity-cards/.

Onalaja, G. (2015). *A Nigerian NGO is suing the NIMC over Mastercard branded national IDs*. TechCabal. https://techcabal.com/2015/03/31/a-nigerian-ngo-is-suing-the-nimc-over-mastercard-branded-national-ids/.

Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of Mixed Methods Research, 4*(1), 56–78.

Osuagwu, P. (2013). *MasterCard grabs Nigeria's identity card deal*. Vanguard. https://www.vanguardngr.com/2013/05/mastercard-grabs-nigerias-identity-card-deal/.

Pandya, J. (2019). Nuances Of Aadhaar: India's digital identity, identification system and ID. Forbes.Com. https://www.forbes.com/sites/cognitiveworld/2019/07/16/nuances-of-aadhaar-indias-digital-identity-identification-system-and-id/?sh=37918bf0209d.

Paradigm Initiative. (2019). *Paradigm initiative calls on NIMC to suspend NIN enforcement activities*. Paradigm Initiative. https://paradigmhq.org/paradigm-initiative-calls-on-nimc-to-suspend-nin-enforcement-activities/.

Privacy International. (2021). Exclusion by design: How national ID systems make social protection inaccessible to vulnerable populations. https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible.

Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2020). Saving face: Investigating the ethical concerns of facial recognition auditing. In *Proceedings of the AAAI/ACM conference on AI, ethics, and society* (pp. 145–151).

SaharaReporters. (2019). Breach of contract: How mastercard used dishonest tactics to edge out chams in million-dollars Nigeria's ID card project. Sahararreporters.Com. http://sahararreporters.com/2019/06/18/breach-contract-how-mastercard-used-dishonest-tactics-edge-out-chams-million-dollars.

Sasu, D.D. (2022) Nigeria: leading social media platforms. [Online] Statista. Available from: https://www.statista.com/statistics/1176101/leading-social-media-platforms-nigeria/ [Accessed 25/03/22].

Stahl, B. C. (2013). Responsible research and innovation: The role of privacy in an emerging framework. *Science and Public Policy, 40*(6), 708–716. https://doi.org/10.1093/scipol/sct067

Stromberg, J. (2014). *Adermatoglyphia: The genetic disorder of people born without fingerprints*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/adermatoglyphia-genetic-disorder-people-born-without-fingerprints-180949338/.

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing, 22*, 960–967.

United Nations (2015) THE 17 GOALS | sustainable development. Available from: https://sdgs.un.org/goals [Accessed 25/03/22].

Unwanted Witness. (2020). Preliminary report Uganda's digital ID system: A cocktail of discrimination. https://www.unwantedwitness.org/download/uploads/UgandaE28099s-Digital-ID-System.pdf.

Vaudenay, S. (2020) Centralized or decentralized? The contact tracing dilemma.

Von Schomberg, R. (2012). Prospects for technology assessment in a framework of responsible research and innovation. *Technikfolgen abschätzen lehren* (pp. 39–61). Springer.

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., & Sperling, O. (2019). *Digital identification: A key to inclusive growth*. McKinsey Global Institute [online].

Whitley, E. A., & Hosein, G. (2010). The challenge of identity policies. *Global challenges for identity policies* (pp. 1–21). Springer.

World Bank. (2019). *Global ID coverage, barriers, and use by the numbers: An in-depth look at the 2017 ID4D-findex survey*. World Bank.