ASSESSING DATA PROTECTION IN NIGERIA:

A look at Biometric Identity, Surveillance, Encryption and Anonymity, and Cybercrimes.

OMIDYAR NETWORK
TECH HIVE ADVISORY
PARADIGM INITIATIVE

Author
Temitayo Ogunmokun

Reviewer and Copy editing
Damilola Ogunmuko

Design and Layout
Kenneth Oyeniyi

This report was written by Tech Hive Advisory, published by Paradigm Initiative with support from Omidyar Network.

Table of Content

Executive Summary **5**
Methodology 9
List of Abbreviations 9

1.0 Introduction **1**

2.0 Status of Data Protection in Nigeria **4**
2.1: Overview of the Legal Framework 4
2.2 International Frameworks 5
2.2.1 ECOWAS Supplementary Act on Personal Data Protection 5
2.2.2 The African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) 5
2.3 Domestic Frameworks 6
2.3.1 The 1999 Nigerian Constitution (As Amended) 6
2.3.2 The Nigeria Data Protection Regulation ("the NDPR") 2019 7
2.3.2 The Nigeria Data Protection Regulation Implementation Framework ("the Framework") 2020 8
2.3.3 Guidelines for the Management of Personal Data by Public Institutions in Nigeria ("the Guideline") 2020 8
2.3.4 The Framework and Guidelines for Public Internet Access (PIA), 2019 8
2.3.5 Cybercrime (Prohibition, Prevention etc.) Act 2015 9
2.4 Sector-Specific Laws 10
2.5 Legislative Efforts 13
a. The Nigeria Data Protection Bill 2020 13
b. NITDA (Amendment) Act 2021 14

3.0 Impact of Legal, Regulatory, and Policy Frameworks across Thematic Areas 16
3.1 Digital and Biometric Identity 16
3.2: Surveillance 19
3.2.1: The Legal and Regulatory Landscape 20
3.3: Encryption & Anonymity 23
3.3.1: The Legal & Regulatory Framework 23
a. Nigerian Data Protection Regulation 2019 23
3.4: Cybercrimes and Cybersecurity: Data Breach and Violations 24

4.0: Major Events on each Thematic Areas 28
4.1: Data Protection Enforcement 28
4.2: Digital and Biometric Identity 29
4.3 Surveillance 33
4.4 Cybercrime and Cybersecurity 35
4.5 Multiple Mandatory Government Registration 37

5.0 Forward-Looking Practices: Safeguards and measures to address regulatory gaps. 41
5.1 Regulatory Gaps 41
5.2 Safeguards and Measures to Address Regulatory Gaps 42

6.0 Recommendations 45

7.0 Conclusion 49

Executive Summary

This report focuses on the impact and effectiveness of the Nigerian data protection regulatory framework across different thematic areas, including digital and biometric identity, surveillance, encryption and anonymity, cybercrime and cybersecurity, and government registration. It comprises an introduction, seven chapters, recommendations, and a conclusion. In addition, the report addresses the following questions:

- What are the data protection violations Nigeria is contending with, and what are the implications and effects?
- How effective are the existing regulatory framework and the role of the regulator?
- What are the significant incidents like policy implementation, court cases, violations, examples of forward-looking practices on data protection?
- What are the guarantees and restrictions through legal provisions (primary or secondary laws) on data protection in the country under review?
- What are the gaps in the existing regulatory framework?
- How do these laws provide for the thematic areas on data protection?
- What is the impact of the current legal, regulatory, and policy requirements framework across the thematic areas?
- What are the measures that can be put in place to address the identified risks?

The first two chapters provide an introduction and overview of the legal framework for data protection in Nigeria, beginning with a brief historical appraisal, challenges accounting for slow legislative developments, the influence of comparative laws and international commitments, and domestic legislation. Next, the chapter traces the earliest attempts at legislation to the draft Computer Security and Critical Information Infrastructure Bill, and the adoption of the Supplementary Act (A/SA.1/01/10) on Personal Data Protection within Economic Community of West African States (ECOWAS), as well as the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), while acknowledging the influence of comparative legislations in other jurisdictions such as the earlier Data Protection Directive and the subsequent General Data Protection Regulation (GDPR) of the European Union's. Finally, the chapter further examines the fragmented status, impact and regulatory conflicts in the domestic framework comprising Section 37 of the Nigerian Constitution, the Nigerian Data Protection Regulation, and relevant sectoral laws in the finance, health, and communication sectors.

The third chapter focuses on the impact of legal, regulatory policy frameworks across specific thematic areas. On digital and biometric identification, the chapter examines the government's efforts to develop a national identification framework, strengthened by the establishment of the Nigerian Identify Management Commission (NIMC) and the regulatory and privacy implications policies concerning digital identity and management. The chapter discusses the legal framework on surveillance, which was initially driven by national cybersecurity and consumer privacy concerns. However, it is now consistently utilised as a legal basis for state surveillance, contrary to domestic and international standards and safeguards. Finally, on encryption and anonymity, the chapter highlights the obligation on the state and organisations to access, utilise and safeguard the private information of citizens reserved in domestic legislations.

On Cybercrimes and Cybersecurity, the chapter highlights the comprehensive regulatory regime created in the Cybercrimes Act as well as the roles of the Cybercrimes Advisory Council (CAC) and the Nigeria Computer Emergency Response Team ("ngCERT"). Finally, on government registration, the chapter highlights the framework for Biometric Voters Registration "("BVR ") adopted by the Independent Electoral Commission of Nigeria INEC through the Advanced Fingerprints Identification System ("AFIS"), as well as the Framework for SIM registration in Nigeria coordinated by the Nigeria Communications Commission (NCC).

The fourth chapter focuses on major enforcement and policy events in each thematic area, emphasising the response and effectiveness of the regulator and the activities of key stakeholders in each context. For example, on data protection, 790 issues were resolved, 15 investigations were conducted into alleged data breaches, seven data controllers were listed for immediate enforcement, and NITDA concluded one investigation. Punitive fines were imposed on Lagos Internal Revenue Service (LIRS), Electronic Settlement Limited (ESL) and Soko Loan Company Limited. On Digital and Biometric Identity, the chapter highlights the presidential approval of the new National Digital Identity Ecosystem Strategic Roadmap for the enrolment of Nigerians and legal residents into the National Identity Database (NIDB) and mandatory the use of the National Identification Number (NIN), which attracted wide public pushback. On surveillance, the chapter explores incidents of surveillance and reports of government use of public resources for the acquisition and deployment of high tech equipment such as the "Stravinsky Project" to spy on citizens.

On Cybercrime and Cybersecurity, the chapter appraises sectoral policies such as the National Cybersecurity Policy and Strategy. On government registration, the

chapter examines policies such as the controversial move to suspend the sale and activation of new SIM cards and the directive of the Minister of Communications and Digital Economy, Isa Pantami, to telecommunication providers instructing the latter to disconnect all mobile telephone lines not linked to valid National Identification Numbers (NINs), with a 2-week compliance deadline for subscribers who were yet to synchronise their SIM cards.

The fifth chapter appraises prominent regulatory gaps in the Nigerian data protection landscape and the measures to remedy them. Despite some progressive initiatives such as the successful launch of the National Digital Economic Policy (NDEPS 2020 – 2030) by President Muhammed Buhari, challenges including regulatory fragmentation, lack of a substantive data protection law, legislative apathy and knowledge of the subject, privacy myopia and non-independence of the regulator, continue to plague the system. Therefore, the chapter proposes the immediate passage of the draft Data Protection Bill to strengthen the framework and cooperation and harmonisation of the data protection landscape.

The six and seventh chapters highlight conclusions and recommendations centred on resolving the confusion around whether Section 37 of the Constitution contemplates data protection by a pronouncement of the supreme or a constitutional amendment, as well as the importance of Nigeria to acknowledge and honour its commitments under regional and sub-regional instruments on data protection or complete the requirements necessary to apply these at a domestic level, especially with the coming into force of the African Continental Free Trade Agreement (AfCFTA). Other recommendations include ensuring the independence of the proposed data protection regulator, i.e. the Data Protection Commission, by removing it from the control of the executive arm of government; raising public awareness on privacy and data protection through training, scholarship, and judicial activism by adopting a multi-stakeholder approach comprising private and public bodies; and review of the legal framework, policies and practices to incorporate the principles of necessity, legality and proportionality and bring them in conformity with international human rights standards.

The report finds that:

1. The continuing fragmentation of the Nigerian data protection regulatory landscape accounts for ambiguity and organisational conflicts with significant socio-economic implications to stakeholders.
2. The industry regulatory, NITDA, has had a slow start but as the 2019-20202 NDPR performance report reflects, it is gradually invoking and applying its

supervisory powers, as evident in the increasing rate of enforcements and draft policies.

3. A substantive Nigerian data protection law that incorporates standard provisions and best practices harmonises the domestic regulatory landscape and establishes an independent supervisory authority must be actualised as soon as possible.
4. A multi-stakeholder approach comprising private and public bodies is required to raise the level of public awareness by committing resources for training, scholarship, lobbying, policymaking, and enforcement of data protection rights.

Methodology

This report employed a qualitative approach**,** including literature review, policy, legal and judicial analysis. In addition, published journals, online and traditional media reports, academic works and governments documents were analysed. This report also incorporated the documented and informed opinions of writers, researchers, academics, civil society organisations, journalists, and human rights advocates.

List of Abbreviations

AFIS	Advanced Fingerprints Identification System
API	Application programming Interface
ARP	Administrative Redress Panel
BVN	Bank Verification Number
BVR	Biometric Voters Registration
CAC	Cybercrimes Advisory Council
CBN	Central Bank of Nigeria
DMB	Deposit Money Banks
DNCR	Department of National Civil Registration
DPA	Data Protection Authority
DPC	Data Protection Commission
DPCO	Data Protection Compliance Organisations
DPO	Data Protection Officers
DSS	Department of State Security
ECOWAS	Economic Community of West African States
EDOCSO	Edo Civil Society Organizations
EFCC	Economic and Financial Crime Commission
EIB	European Investment Bank
EU	European Union
FGN	Federal Government of Nigeria
FGN	Federal Government of Nigeria
FMCDE	Federal Ministry of Communications and Digital Economy
FMI	Federal Ministry of Interior
GDPR	General Data Protection Regulation
INEC	Independent National Electoral Commission
ISSC	Information Security Steering Committee
LIRS	Lagos Internal Revenue Service
NCC	Nigerian Communications Commission

NCPS	National Cybersecurity Policy and Strategy
NDEP	National Digital Economic Policy
NDPR	Nigerian Data Protection Regulation
NeFF	Nigerian Electronic Fraud Forum
NIDB	National Identity Database (NIDB)
NIMC	National Identity Management Commission
NIN	National Identification Number
NITDA	Nigerian Information Technology Development Agency
OSIA	Open Standards Identity APIs
PIAP	Public Internet Access Providers
PVC	Permanent Voter Cards
SIM	Subscriber Identity/Identification Module
USSD	Use of Unstructured Supplementary Service Data

1.0

Introduction

Data is the raw resource with which information and knowledge are generated. It is the fuel that powers different business activities, particularly in the digital economy, and is a major driver of globalisation. [1] As the largest economy and population in Africa, Nigeria is not left out of the effects of the utilisation of this asset. [2] As the digital economy burgeons, the demand for the personal data of Nigerians by private and public stakeholders is witnessing an unprecedented surge. The processing of personal data on a mass scale is especially necessary for establishing, monitoring, and maintaining national infrastructure on digital and biometric identity, security surveillance, cybersecurity, government registration, freedom of expression, and other matters of national concern. In the absence of effective regulatory frameworks for these activities, abuse is inevitable, with grave economic and personal consequences for stakeholders.[3]

Globalisation is driving the adoption of data reliant IT infrastructure and services in Nigeria, a development highlighted by the level of internet and telecommunication penetration. Statistics show that internet penetration stood at about 61.2%, with 98% of the adult population having access to a mobile phone. The digital economy accounted for 17.8% of the Gross Domestic Product (GDP) in 2020.[4] As the rest of the world increasingly leverages technology and data flow to stimulate national and international development, the importance of an organised framework for regulating the use of data becomes more apparent, hence driving the notions of privacy and data protection to the fore. While many jurisdictions have designed and implemented relevant models, the most influential and comprehensive is the European 'Union's General Data Protection Regulation (GDPR)[5]; Nigeria appeared

[1] The Economist (6 May 2017): "The world's most valuable resource is no longer oil, but data", https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data accessed on 25 August 2021

[2] According to the World Bank, Nigeria's GDP for the year 2020 was 432.30 billion US dollars. See also Adedayo Akinwale and Dike Onwuamaeze (5 March 2020): "Nigeria Overtakes South Africa As Africa's Largest Economy", https://allafrica.com/stories/202003050216.html, accessed on 25 august 2021

[3] Chinerem Ubaka (12 December 2020): Data Protection in Nigeria: How Has the Journey Been?" https://www.linkedin.com/pulse/data-protection-nigeria-how-has-journey-been-chinecherem-ubaka/, accessed on 26 August 2021

[4] NITDA: "Nigeria Data Protection Regulation Performance Report 2019-2020", pg 9 http://www.nitda.gov.ng/wp-content/uploads/2021/03/NDPR-Lite-Performance-Report-2019-2020.pdf, accessed on 23 August 2021

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/E.C. (General Data Protection Regulation)

to have adopted a laidback approach to this issue until recently. However, the country made a bold statement to strengthen its data protection framework and raise it to international standards by releasing the Nigerian Data Protection Regulation (NDPR). Although this is a subsidiary legislation, it remains its most comprehensive piece of law on the subject to date.[6] The NDPR draws significant influence from the 'EU's General Data Protection Regulation and mirrors it in language, objectives, scope, compliance obligations, and enforcement framework. With the passing of the NDPR, Nigerian became one of the countries to regulate data protection on the African continent.[7]

However, while the NDPR makes provisions for key issues such as data processing principles, lawful bases, data 'subjects' rights, cross border data flows, enforcement mechanisms, among other issues, concerns over the adequacy and effectiveness of the legislation have been expressed by stakeholders.[8] Some of these concerns are accentuated by the fragmented regulatory landscape of the Nigerian data protection landscape and the subsidiary nature of the NDPR. The NDPR is a skeletal imitation of the 'EU's General Data Protection Regulation. However, the latter law manifestly embodies the spirit, principles and idiosyncrasies that underpin the European Union as a distinct, supranational legal order. Therefore, while the standards established in the GDPR are admirable, it is doubtful whether the NDPR takes cognisance of national peculiarities, history and requirements, a flaw usually exposed in attempts at enforcement.

Furthermore, the absence of a holistic and substantive Nigerian data protection law constrains recourse to many sectoral laws for specific issues touching on data protection, hence bringing stakeholders under the scope of different and sometimes conflicting legislation and regulators. The bureaucracy, lack of clarity and issues of conflict of laws arising from this trend are drawbacks to the successful implementation, monitoring and administration of the domestic data protection framework. Hence, reports of regulatory gaps, vagueness, violations, breaches and lack of enforcement are commonplace, often to the detriment of the biggest stakeholders, i.e. data subjects.[9]

---

[6] Hunton Andrews Kurth (5 April 2019): "Nigeria Issues New Data Protection Regulation", https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/, accessed on 26 August 2021

[7] Brian Daigle: Data Protection Laws in Africa: A PanAfrican Survey and Noted Trends, United States International Trade Commission Journal of International Commerce and Economics, pg8

[8] Diyoke Michael Chika1, Edeh Stanley Tochukwu: An Analysis of Data Protection and Compliance in Nigeria, International Journal of Research and Innovation in Social Science (IJRISS) |Volume IV, Issue V, May 2020|ISSN 2454-6186, Pg 2

[9] Ibid

Given the foregoing, this report will attempt an assessment of the Nigerian data protection landscape, taking into account the current set-up; common violations and their implications; gaps, guarantees and restrictions; effectiveness of the existing framework, and the role of the regulator; risk identification, mitigation and resolution. This report will also highlight the impact of legal, regulatory, and policy frameworks and major events across thematic areas (digital and biometric identity, surveillance, cybersecurity, encryption and anonymity, voter registration, sim registration and freedom of expression, and conclude with recommendations on forward-looking safeguards and practices.

2.0

Status of Data Protection in Nigeria

2.1: Overview of the Legal Framework

The recognition of data protection as a subject of regulation in Nigeria was driven by developments in technology and the digital economy [10] and comparative legislative activities of other jurisdictions.[11] However, despite the efforts at regulation, data protection in Nigeria has a chequered history, plagued with poor record-keeping, judicial apathy, and political wrangling. Some experts opine that the first real attempt to regulate data protection was the Computer Security and Critical Information Infrastructure Protection Bill 2005. This is arguable as the Bill primarily sought to criminalise illegal conduct against ICT systems and cybercrimes, among other objectives.[12]

Due to the absence of a holistic domestic data protection law of comparative broadness as obtained in the European Union and other jurisdictions, Nigeria's current data protection landscape is fragmented, comprising primarily of subsidiary legislation, the NDPR, and other sectoral laws. The assortment of legislation on data protection accounts for gaps in the framework, regulatory encroachment, and lack of clarity. It is believed that some of these gaps can only be rectified by the passage of a substantive data protection law that takes domestic cognisance of domestic needs and peculiarities while matching international standards.[13] In addition, the Nigerian data protection framework also draws life and influence from certain international legal regimes further examined in this report. However, many broad and sectoral laws intended to regulate data protection in Nigeria are still at the draft level.[14]

---

[10] Babalola, Olumide, A Bird's Eye Rundown on Nigeria's Data Protection Legal and Institutional Model (March 20, 2021). Available at SSRN: https://ssrn.com/abstract=3808570 pp. 2

[11] Alex B. Makulilo, 'The Quest for Information Privacy in Africa' (2018) 8 Journal of Information Policy, pp. 317.

[12] Oluwafemi Jemilohun and Ifedayo Akomolede, "Regulations or Legislation for Data Protection in Nigeria? a call for a clear Legislative Framework", Global Journal of Politics and Law Research Vol.3, No. 4, pp.1-16, August 2015, https://www.eajournals.org/wp-content/uploads/Regulations-or-Legislation-for-Data-Protection-in-Nigeria1.pdf, accessed 27 August 2021

[13] See Dike Ibegbulem, 'The Protection of Consumers' Personal Data in the Era of e-Commerce in Nigeria' (2019), https://www.researchgate.net/publication/334837471_The_Protection_of_Consumers'_Personal_Data_in_the_Era_of_E-commerce_in_Nigeria , accessed 21 August 2021

[14] E.g. See the NITDA Amendment Act 2021, Electronic Communications and Transactions Bill 2009; Electronic Commerce (Provision of Legal Recognition) Bill of 2008; and the Digital Rights and Freedom bill 2017.

2.2 International Frameworks

2.2.1 ECOWAS Supplementary Act on Personal Data Protection[15]

The Supplementary Act is a legally binding law adopted at the 37th session of the authority of Heads of State and Government in Abuja in February 2010 by the Nigerian government and other states in the community. It specifies the content of data protection laws, regulates the processing of personal data by private and public authorities, and mandates establishing independent Data Protection Authorities by member states.[16] However, while the law is technically considered a part of the Nigerian data protection framework, it has not been domesticated by the legislature as of July 2021 and therefore lacks binding effect by the operation of Section 12 of the Nigerian Constitution.[17]

2.2.2 The African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)

To address the growing challenges posed by cybersecurity and cybercrime, the African Union in 2014 passed the Malabo Convention to establish a 'credible framework for cybersecurity in Africa through the organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.'[18] The Convention targets three main areas, i.e. protection of personal data, electronic transactions, and cyber security and cybercrime. It mandates member states to establish legal frameworks, strengthen fundamental rights, protect the personal data of natural personal data while facilitating the seamless transfer of data across national borders.[19]

The Convention is regarded as the first attempt to establish the semblance of a harmonised data protection framework across the African continent and is slated to come into operation upon ratification by 15 member states.[20] However, as of July 2021, only eight states have ratified the Convention, excluding Nigeria. Nigeria has

[15] Supplementary Act A/SA.1/01/10 ON Personal Data Protection Within Economic Community of West African States (ECOWAS)

[16] Greenleaf, Graham, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108 (October 19, 2011)," International Data Privacy Law, Vol. 2, Issue 2, 2012; UNSW Law Research Paper No. 2011-39; Edinburgh School of Law Research Paper No. 2012/12.

[17] Olumide Babalola, ibid p 3

[18] Kriangsak Kittichaisaree: Public International Law of Cyberspace, 2017, Volume 32 ISBN : 978-3-319-54656-8, pg 6Bottom of Form

[19] Article 8 (1)(d) id.

[20] Article 36 id.

neither signed nor ratified it; therefore, it has no binding effect in Nigeria at the moment.[21]

2.2.3. Declaration of Principles of Freedom of Expression and Access to Information in Africa

Declaration of Principles of Freedom of Expression and Access to Information in Africa by the African Commission on Human and People's Rights provides a set of enhanced normative standards for freedom of expression, access to information and digital rights in Africa, in line with international human rights and standards.[22] In addition, the Declaration provides Principles that member states have been encouraged to adopt. For example, principle 40 provides privacy and protection of personal information, while Principle 41 addresses communications surveillance. Finally, Principle 43 provides guidance on the legal framework for protecting personal information, which includes the establishment of independence for the data protection authority.

2.3 Domestic Frameworks

2.3.1 The 1999 Nigerian Constitution (As Amended)

The 1999 Constitution in Section 37 provides for "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected". However, unlike the specific provisions on the fundamental rights of privacy and data protection in the constitutional documents of a country like Argentina[23] or the European Union[24], the Nigerian Constitution makes no such distinction and does not expressly mention data protection nor provide for its protection. As a result, scholarly opinions and judicial arguments differ on whether Section 37 provides a constitutional basis for

[21] Only 8 member states i.e. Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwandan and Senegal, have ratified the Malabo Convention so far.

[22] Centre for Human Rights, African Commission Publishes Revised Declaration of Principles of Freedom of Expression and Access to Information in Africa amid COVID-19 Crisis - Centre for Human Rights" (*Up.ac.za*April 23, 2020) <https://www.chr.up.ac.za/expression-information-and-digital-rights-news/2056-african-commission-publishes-revised-declaration-of-principles-of-freedom-of-expression-and-access-to-information-in-africa-amid-covid-19-crisis> accessed November 26, 2021.

[23] Adrian Furman and Francisco Zappa, The Law Reviews - the Privacy, Data Protection and Cybersecurity Law Review (*Thelawreviews.co.uk*2021) <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/argentina> accessed November 26, 2021.

[24] See Article 16 of the Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01

data protection.[25] However, in the first appellate resolution of the subject in Nigeria, the Court of Appeal recently provided some direction by holding that data protection falls within Section 37.[26] It is hoped that the legislature will provide definite and conclusive clarity on this issue, but until then, the prevalent opinion appears to be that Section 37 serves as a constitutional basis for data protection.[27]

2.3.2 The Nigeria Data Protection Regulation ("the NDPR") 2019

The publication of the Nigerian Data Protection Regulation[28] by the National Information Technology Development Agency's (NITDA) on the 25th of January 2019 changed the data protection landscape in Nigeria[29]. NITDA's attempt at regulating data protection started in 2013 with the Draft Guidelines on Data Protection[30]; the Agency followed it by releasing another Data Protection Guidelines in 2017. The NDPR was issued under section 6 (a) and (c) of the National Information Technology Development Agency Act 2007 (the 'NITDA 'Act') and is administered by the NITDA, which plays the role of the Data Protection Authority (DPA) in Nigeria.

The preamble to the NDPR broadly spells out its significance and objectives. It applies to all transactions intended for the processing of personal data, notwithstanding how the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria.[31] The NDPR establishes the governing principles of data processing in Nigeria, the lawful basis for processing, the rights of data subjects, cross border transfer rules, contents of a privacy policy and implementation mechanisms. The NDPR also established the Administrative Redress Panel (ARP) to investigate allegations of any breach of the NDPR,

[25] See the unreported decisions in Suit No. FHC/AB/CS/85/2020 between Digital Rights Lawyers Initiative and Unity Bank and Suit No. FHC/AB/CS/ 79 between Laws and Rights Awareness Initiative and National Identity Management Commission delivered in December 2020 and Suit No. H.C.T./262/2020 between Incorporated Trustees of Digital Rights Lawyers Initiative Digital Rights Lawyers Initiative and LT Solutions Media Ltd)

[26] See Incorporated Trustees of Digital Rights Lawyers Initiative and National Identity Management Commission, Suit No. CA/IB/291/2020. Full judgement can be read via https://drive.google.com/file/d/1BsddOfWSHNk7h4R2ZJ8WIARQe9BrfHUm/view, accessed on 6 October 2021

[27] Francis Ololuo (19 February 2020): Nigeria: Data Privacy And Protection Under The Nigerian Law, published on https://www.mondaq.com/nigeria/privacy-protection/895320/data-privacy-and-protection-under-the-nigerian-law, accessed 23 august 2021

[28] Hereinafter NDPR

[29] Emma Okonji (22 August 2019): Divergent Views Trail NITDA's Data Protection Regulation", https://www.thisdaylive.com/index.php/2019/08/22/divergent-views-trail-nitdas-data-protection-regulation/, accessed on 26 August 2021

[30] Uche Val Obi (9 September 2020), 'An Extensive Article on Data Privacy and Data Protection Law in Nigeria' https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/ accessed on 30 July 2021. Note also that NITDA published another set of draft guidelines in 2017. See Chukwuebere Ebere Izuogu (18 October 2018): "Whiter the NITDA Data Protection Guidelines 2017?", https://www.linkedin.com/pulse/whiter-nitda-data-protection-guidelines-2017-chukwuyere-ebere-izuogu/, accessed 30 July 2021

[31] Paragraph 1.2. of the NDPR

adjudicate disputes and issue administrative orders.[32] Although the validity of the Regulation has been questioned on the ground that the NITDA Act does not directly or indirectly empower NITDA to issue such a Regulation[33] and that the 'NDPR's status as a delegated legislation and a stop-gap measure continues to hamper its enforcement,[34] nevertheless, it remains the primary body of law regulating data protection in Nigeria.

2.3.2 The Nigeria Data Protection Regulation Implementation Framework ("the Framework") 2020

The NDPR Implementation Framework was issued in November 2020 by NITDA to promote contextual clarity and voluntary compliance with the NDPR. The framework is to be read in conjunction with the NDPR and other applicable laws but does not supersede the NDPR. It clarifies provisions of the NDPR such as consent, cross-border transfer of data, privacy breaches, data protection audit, the roles of Data Protection Officers ("D.P.O.s") and Data Protection Compliance Organisations ("DPCOs"), the establishment of the administrative Redress Panel among other things.

2.3.3 Guidelines for the Management of Personal Data by Public Institutions in Nigeria ("the Guideline") 2020

NITDA issued this in May 2020 as a Guideline for implementing the NDPR within Public Institutions in Nigeria. The purpose of the Guideline is to guide Public Officers on handling and managing personal information in compliance with the NDPR.[35] The Guideline applies to all public institutions in Nigeria, including departments, ministries, publicly funded ventures, agencies, public corporations, institutions, and incorporated entities with government shareholding, at the state or local, state and federal levels, while collecting and processing personal data.[36]

2.3.4 The Framework and Guidelines for Public Internet Access (PIA), 2019

The PIA mandates the Public Internet Access Providers (PIAPs) to adhere to all the provisions of the framework as listed in the Guidelines in the provision of public internet access. In addition, PIAPs are charged to ensure that every online

[32] Paragraph 4.2 ibid

[33] Oluwafemi Jemilohun and Ifedayo Akomolede, ibid

[34] World Bank Group. 2019. Nigeria Digital Economy Diagnostic Report. Washington, DC: World Bank. License: Creative Commons Attribution CC BY 3.0 IGO https://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf, accessed on 23 July 2021

[35] Paragraph 1.2 of the Guidelines

[36] Paragraph 1.4 ibid

communication is encrypted[37] and to ensure the protection of users' data and that user privacy is adhered to in line with Data Protection Guidelines 2018.[38]

2.3.5 Cybercrime (Prohibition, Prevention etc.) Act 2015[39]

Although the Cyber Crimes Act ("the Act") is not a data protection instrument in the strict sense, the Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the "prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The law primarily aims to "promote cybersecurity and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights". [40] Section 38 of the act provides that

> "Anyone exercising any function under this section shall have due regard to the 'individual's **right to privacy** under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the **confidentiality of the data retained, processed or retrieved** for the purpose of law enforcement". "[41]

Accordingly, the Act only addresses data protection when it intersects with cybercrimes. However, the ECOWAS Court in July 2020, ruled that the federal government should repeal the Cybercrimes Act for violating freedom of expression and its commitment under international human rights norms.[42] A suit was filed challenging provision of Section 24 of the Act for being vague which could lead to arbitrary abuse of the provision. Similar law suit brought before the Nigerian court rejected the argument.[43]

Other laws that reflect provisions on data protection include the Child Rights Act 2003, Labour Act 1990, Police Act 2020, Companies and Allied Matters Act (CAMA) 2020, Federal Competition and Consumer Protection Act (FCCPA) 2018, Freedom

---

[37] See Rule 3.1.V ibid

[38] Rule 3.1 VII ibid

[39] Cited as the Cybercrime (Prohibition, Prevention etc.) Act 2015

[40] Section 1(c) ibid

[41] Section 38 (5) ibid

[42] Ade Adesomoju, ECOWAS Court Orders FG to Repeal Cybercrime Law - Punch Newspapers" <https://punchng.com/ecowas-court-orders-fg-to-repeal-cybercrime-law/#:~:text=The%20ECOWAS%20Court%20of%20Justice,violates%20citizens'%20right%20of%20expression.> accessed November 26, 2021.

[43] Okedara v. Attorney General - Global Freedom of Expression <https://globalfreedomofexpression.columbia.edu/cases/okedara-v-attorney-general/> accessed November 26, 2021.

of Information Act 2011, Credit Reporting Act, National Health Act, Hiv/AIDS Discrimination Act, Guidelines and Regulations by the Nigeria Communication Commission (NCC), Guidelines and Regulations by the Central Bank of Nigeria (CBN) etc.

2.4 Sector-Specific Laws

Certain industry-specific laws also reflect provisions that regulate the processing of personal within the sector:

2.4.1 Health Sector:

- The National Health Act ("NHA.")[44] 2014 provides for a lawful basis for disclosing medical and health data[45] and mandates health providers to put in place control measures to prevent unauthorised access to medical records in the storage facility.[46]

  The HIV and AIDS Anti-Discrimination Act 2014 prohibits the disclosure of the medical status of infected persons without their consent[47], provides for anonymous testing on request and confidentiality of medical data processed in the course of testing.[48]
- Guidelines on Document and Record Retention developed by the Medical Laboratory Science Council of Nigeria provide different retention periods for different health data categories.

2.4.2 Financial Sector:

The Central Bank of Nigeria - performs regulatory oversight in the Nigerian financial sector through the CBN Act 2007 and subsidiary regulations.

- The Central Bank of Nigeria ("CBN") Guidelines on Mobile Money Services 2021 mandates mobile money operators to retain records of transactions on their platform for a minimum of 3 years and subsequently archive these records for a minimum period of seven (7) years.[49] The Guidelines also

[44] National Health Act (Act No. 8, LFN 2014)

[45] Sections 27 &28 ibid

[46] Section 29 ibid

[47] Cited as the HIV and AIDS (Anti-Discrimination) Act 2014

[48] Section 13 ibid

[49] Paragraph 16.0 of the Mobile Money Services Guidelines

provides for the minimum security standards Mobile Money operators must maintain[50] alongside ensuring the confidentiality and privacy of customers.

- The CBN Supervisory Framework for Payment Service Banks ("PSBs") in Nigeria 2021 mandates PSBs to put prescribed minimum standards for Data Infrastructure and cybersecurity in place.[51]

- The CBN Regulatory Framework for the Use of Unstructured Supplementary Service Data ("USSD") for Financial Services in Nigeria 2018 provides data security and risk mitigation in deploying USSD technology in Financial Services.

- The Credit Reporting Act 2017 provides that Data subjects have the right to privacy, confidentiality and protection of their Credit Information[52] and that the Credit Bureau shall not disclose information relating to Data Subjects to Credit Information Users without obtaining the Data Subject's written consent.[53]

- The CBN Regulatory Framework for Bank Verification Number "("BVN"") Operations and Watch-List for the Nigerian Banking Industry 2017 has one of its objectives: defining access, usage, and management of the BVN information, requirements, and conditions.[54]

- The CBN Consumer Protection Regulation 2019 imposes an obligation on financial institutions to maintain the confidentiality and privacy of all financial services customers – present or past.[55]

- The CBN Guidelines on Transaction Switching Services, 2016 provides a framework for switching services in Nigeria, including the rights and obligations of the parties to the switching contract. In addition, the Guidelines mandate the protection of the privacy and information of cardholders[56] and prescribe minimum standards of security and compliance with PCI Data Security Standards (DSS).[57]

---

[50] Paragraph 16.0 ibid

[51] Paragraph 9.0 of the Payment Service Banks Framework

[52] Section 9 (1) of the Credit Reporting Act

[53] Section 9 (2) (b) (ii) ibid

[54] Paragraph 1.2 (iii) of the BVN Framework

[55] Paragraph 5.4 of the Consumer Protection Regulation

[56] Rule 1.7 ibid

[57] The Guidelines compel Switching Companies to retain their transaction database for a minimum period of 7 years. See Rule 2.2.3

- Money Laundering (Prohibition) Act 2003 requires certain (financial) service providers to retain transaction records, including customers' identities, for a minimum of ten (10) years.[58]

2.4.3 Communications Sector:

- Nigerian Communications (Enforcement Process etc.) Regulation 2019 stipulates a data retention period of two years for telecommunication service providers.[59]

- Guidelines for Nigerian Content Development in Information and Communication Technology 2019 mandates adopting data security measures prescribed by the Guidelines and localisation of data by data and information management firms.[60]

- NCC Internet Code of Practice 2019, which regulates the activities of Internet Service Providers (I.S.P.s), provides for transparency, data security and breach notification procedures. [61]

- NCC (Registration of Telephone Subscribers) Regulations recognise section 37 of the Constitution and contain Data Protection and Confidentiality provisions, particularly in the Central Database.[62]

- NCC. Consumer Code of Practice Regulations 2007 provides for general principles and implements a Protection of Consumer Information Policy. [63]

- Lawful Interception Communications Regulation 2019 provides the regulatory framework for communications surveillance in Nigeria. It addresses the legal safeguards required for surveillance.

[58] Section 3(2), 7(a) and (b) of the Money Laundering Act

[59] Paragraph 8(1) of Nigerian Communications (Enforcement Process etc.) Regulation

[60] Paragraph 14 of the Guidelines for Nigerian Content Development in Information and Communication Technology

[61] Paragraph 3.1 and 4 of the NCC Internet code of Practice

[62] Regulation 9 (2) & (4) of the NCC Registration of Telephone Subscribers Regulations

[63] Regulation 34-38 of the NCC. Consumer Code of Practice Regulations

2.4.4 Insurance Sector

- Nigerian Insurance Industry ICT Guideline created different obligation**s** on insurance companies to ensure the privacy and security of data they process. Specifically, they are expected to comply with the NDPR.[64]
- Market Conduct and Business Practice Guideline for Insurance Institutions in Nigeria imposes the obligation on insurance companies to ensure security and privacy in the industry.[65]

2.5 Legislative Efforts

a. The Nigeria Data Protection Bill 2020

As part of ongoing efforts to modernise 'Nigeria's data protection landscape, concrete steps are being taken to create reforms and actualise the passage of a substantive Data Protection Act in place of the failed Protection of Personal Information Bill 2016 and the 2019 Data Protection Bill).[66] The reforms are driven on behalf of the national government by the Legal and Regulatory Reform Working Group of the Digital Identity Ecosystem Project, which consists of representatives of the Ministry of Justice, FMCDE, NIMC, NITDA, NCC, National Population Commission, NIS, Office of the Secretary to the Federal Government and the Independent National Electoral Commission (INEC)[67]. The Working Group is tasked with upgrading the regulatory framework for identity management in the country.[68]

A draft of the Data Protection Bill 2020 was published on the 19th of August 2020, a sequel to public consultation for comments from the public. The Bill was also displayed across nine websites to ease accessibility and even distribution of the Bill to obtain inputs from stakeholders and other interested persons.[69] The Bill establishes a Data Protection Authority known as the Data Protection Commission

[64] REVIEW of the NIGERIAN INSURANCE INDUSTRY ICT GUIDELINE (N3IG 1.0) VERSION 1.0 <https://techhiveadvisory.org.ng/wp-content/uploads/2021/03/REVIEW-OF-THE-NIGERIAN-INSURANCE-INDUSTRY-ICT-GUIDELINE.pdf> accessed October 22, 2021.

[65] Paragraph 1.9.0 of Market Conduct and Business Practice Guideline for Insurance Institutions in Nigeria

[66] The Council of Europe, in conjunction with the Federal Ministry of Justice and some other stakeholders, drafted the Nigerian Data Protection Bill 2018. The Bill was finally presented to the law President for presidential assent. Unfortunately, the President refused to grant assent.

[67] African Declaration on Internet Rights and Freedoms Coalition (APC), 20 May 2021: Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries, pp 189

[68] Nasiru, J. (2020, 14 September) The Cable https://www.thecable.ng/fg-data-protection-law-will-help-us-gain-trust-of-nigerians , accessed on 27 August 2021

[69] Data Guidance "Nigeria: Notable Provisions of the Data Protection Bill 2020 Amid Public Consultation", https://www.dataguidance.com/opinion/nigeria-notable-provisions-data-protection-bill-2020-amid-public-consultation, accessed on 2 August 2021

(DPC), a conspicuously absent feature in the NDPR.[70] It generally applies to Data Subjects who are citizens of Nigeria, resident in Nigeria, a body incorporated under Nigerian law, an unincorporated joint venture or association operating in part or whole in Nigeria, any person who maintains an office, branch or agency through which business activities are carried out in Nigeria and Foreign entities targeting persons resident in Nigeria.[71] It contains provisions on the Principles for processing data, legal bases for the processing, duties of Data Controllers and Data Processors, trans-border flow of personal data, offences and penalties, among other things. However, the Bill is conspicuously silent on the status of the NDPR.

b. NITDA (Amendment) Act 2021

There are also reports on proposed amendments to the current NITDA Act. The proposed amendment Bill allegedly contains some controversial provisions which grant the Agency broad powers, including the authority to "enter premises, inspect, seize, seal, detain and impose administrative sanctions on erring persons and companies who contravene any provision of the Act subject to the order of a court of competent jurisdiction". It also seeks to introduce a new regime of licenses and penalties.[72] However, the proposed amendments have been greeted with criticisms from several quarters as the Bill was allegedly drafted without the input of major stakeholders or presented to the NITDA board for discussion or approval.[73] In any event, it is yet to be presented before the National Assembly for deliberations.

c. Other developments

In November 2021, the government issued an advert requesting expression of interest to draft a new data protection Bill and subsidiary regulations.[74] The advert suggests that the government is jettisoning the Data Protection Bill 2020, which means the ongoing effort will be abandoned and restarted. Similarly, the lack of a federal legislature enacted data protection law has encouraged state governments to enact their laws. Lagos State is taking the lead with its Data Protection Bill that

[70] Section 7 of the Data Protection Bill 2020

[71] Section 2 (3) ibid

[72] Ogheneruemu Oneyibo (Aug 19, 2021): 11 Critical Questions on the Leaked NITDA Bill; A Tussle for More Power? https://techpoint.africa/2021/08/19/leaked-nitda-bill/ accessed on 29 august 2021

[73] Lucas Ajanaku (19 August 2021): NCS kicks against proposed amendment to NITDA Act, https://thenationonlineng.net/ncs-kicks-against-proposed-amendment-to-nitda-act/ accessed on 28 August 2021

[74] Tosin Omoniyi, "Data Protection: Indignation as FG Abandons Draft Bill, Seeks 'Consultants' for Fresh Process" (*Premium Times Nigeria*November 17, 2021) <https://www.premiumtimesng.com/news/top-news/495768-data-protection-indignation-as-fg-abandons-draft-bill-seeks-consultants-for-fresh-process.html> accessed November 26, 2021.

recently scaled the second reading[75], and the parliamentary committee on science and technology held a public hearing.[76] A similar legislative proposal is being mooted in Ogun State, and it could be a trend other states might adopt. The challenge with the multiplicity of effort is the lack of common standards that could create operationalisation chaos, increase organisations' compliance landscape, and offer little to protect human rights.

[75] Lagos Data Protection Bill Scales Second Reading (*Premium Times Nigeria*October 25, 2021) <https://www.premiumtimesng.com/regional/ssouth-west/491701-lagos-data-protection-bill-scales-second-reading.html> accessed November 26, 2021.

[76] Victor Ayeni, "Assembly Moves to Protect Lagosians' Data from Unauthorised Usage - Punch Newspapers" (*Punch Newspapers*November 18, 2021) <https://punchng.com/assembly-moves-to-protect-lagosians-data-from-unauthorised-usage/> accessed November 26, 2021.

3.0

Impact of Legal, Regulatory, and Policy Frameworks across Thematic Areas

3.1 Digital and Biometric Identity

The efforts taken by the Federal Government of Nigeria ("FGN") to develop national identification is over 40 years old. The Department of National Civil Registration ("DNCR") was established within the Federal Ministry of Interior (FMI) in 1978 and tasked with issuing national identity cards. In 2001, DNCR contracted a private partner to enrol people and issue national identity cards at a fiscal cost of US$236.8 million. The program ran for five (5) years, and national identity cards were issued to 37.3 million people before it was abruptly shelved. Nigeria's current digital identity landscape is traceable to the National Identity Management Commission (NIMC) Act,[77] which established the National Identity Management Commission (NIMC) and empowered it as the industry regulator. The NIMC collects and maintains the identities of citizens and aliens in Nigeria in a National Identity Database.[78]

Former President, Goodluck Jonathan, launched the pilot phase of the e-ID scheme on the 28th of August 2014 to issue electronic ID. The ID cards would serve the dual functions of identity and payment cards. Since registration commenced, well over 59 million people have been biometrically enrolled for the National Identification Number (NIN) as of July 2021.[79] Today, about fifteen federal offer identification services in Nigeria with overlapping functions and significant cost implications.[80]

S/N	Ministry, Department or Agency ("MDA.")	Functions
1.	Central Bank of Nigeria **("CBN")**	Operates and maintains the database of people who use banking services in Nigeria

[77] National Identity Management Commission (NIMC) Act 2007 No 23. LFN 2004

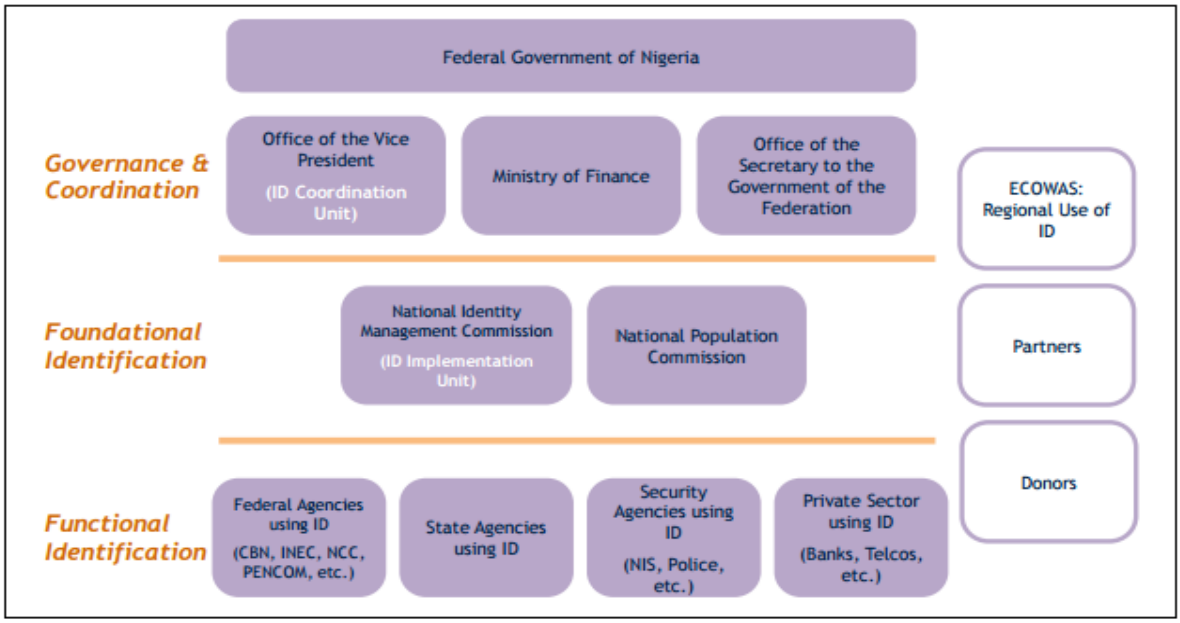
[78]National Identit

[79]y Management Commission (NIMC) Act 2007 No 23. LFN 2004
rollment for digital ID nears 60M on telco boost" https://www.biometricupdate.com/202107/nigeria-biometric-enrollment-for-digital-id-nears-60m-on-telco-boost, accessed on 9 July 2021

[80] Awodele Olubusayo et al.: "An Overview of Digital Identity and Digital Identification in Nigeria", Digital Rights Lawyers' Publications, January 2021, pg 23

2.	Independent National Election Commission ("**INEC**")	Operates and maintains the database of eligible voters in Nigeria
3.	National Communications Commission ("**NCC**")	Operates the registry of mobile phone users in Nigeria
4.	National Health Insurance Scheme ("**NHIS**")	Operates the registry of people who subscribe to health insurance in Nigeria
5.	Federal Inland Revenue Service ("**FIRS**")	Operates the registry for taxpayers in Nigeria and for Nigerians in the diaspora liable to pay tax in Nigeria
6.	Joint Tax Board (Customs)	Operates the registry of people for excise and customs duties in Nigeria
7.	National Pensions Commission ("**PENCOM**")	Operates and maintains the registry of persons entitled to pension by the Federal Government of Nigeria
8.	National Social Safety Net Project ("**NASSP**")	Operates and maintains the database of the indigent and vulnerable people in Nigeria
9.	Federal Ministry of Agriculture and Rural Development ("**FMARD**")	Operates and maintains the database of farmers entitled to agriculture benefits from the FGN.
10.	National Immigration Service ("**NIS**.")	Operates the registry of people with a valid Nigeria passport or other travel documents
11.	Federal Road Safety Corps ("**FRSC**")	Operates a registry of persons licensed to drive in Nigeria
12.	Nigeria Population Commission ("**NPC**")	The lead agency tasked with registering births and deaths in Nigeria
13.	Nigeria Identity Management Commission ("**NIMC**")	The custodian of the National Identity Management System and database under Nigerian law
14	Nigeria Correction Service (NCoS)	Operates and maintain a biometric database of all prisoners.
15	National Home Grown School Feeding Programme (NHGSFP)	Responsible for running the school feeding program of the government.

The Federal Executive Council (FEC) of Nigeria subsequently approved a Strategic Roadmap for Developing Digital Identification in Nigeria to forge a credible and cost-effective pathway for identification management.[81] The Nigerian government also established a steering committee to oversee the adoption of a harmonised Digital Identity for Nigerians, a strategic unit, and an implementation unit situated in the NIMC. The committee would aim to harmonise data such as the Bank Verification Number (BVN), 'driver's license, international passport, and the National Identity Number (NIN) held by various government bodies. In addition, a Digital Identity Ecosystem powered by the NIMC and involving public and private service-providing partners was also established for the effective and efficient mass enrolment of Nigerians and legal residents in Nigeria into a consolidated, secure National Identity Database where everyone is issued with digital identities in the form of the National Identity Number (NIN).



Digital Identity Ecosystem image courtesy of 'A Strategic Roadmap for Developing Digital Identification in 'Nigeria' report

As part of the Strategic Roadmap, The Nigeria Digital Identification for Development (ID4D) Project was developed by the Nigerian Federal Government in partnership with the Agence Française de Developpement (AFD), World Bank, and European Investment Bank (EIB). The project comprises four components: (1) Strengthening the Legal and Institutional Framework (2) Establishing a Robust and Inclusive Foundational ID System (3) Enabling Access to Services through IDs (4)

[81] National Identification Commission of Nigeria (12 September 2018): "A Strategic Roadmap for Developing Digital Identification in Nigeria" http://citizenshiprightsafrica.org/a-strategic-roadmap-for-developing-digital-identification-in-nigeria/ accessed on 18 August 2021

Project Management and Stakeholder Engagement, and aims to support the FGN to implementing best practices and achieve key objectives for universal ID and CR systems, considering privacy implications.[82]

The European Investment Bank (EIB) is also financing a "Nigeria Digital ID" project which envisages the "development of a digital identity (eID) infrastructure in Nigeria and the supply of a biometric identity to all Nigerian citizens" in Nigeria and the diaspora, at an approximate cost of €706 (Seven Hundred and Six Million Euros).[83] The project is intended to strengthen 'Nigeria's digital economy, improve access to mobile phones, liberalise e-banking services and drive the provision of innovative products and services to consumers. The 'project's activities consist of upgrading IT systems in existing data centres and collecting data from the population for providing them with a digital ID. The EIB will rely on the World Bank, acting as the lead financier, to ensure the project implementation is performed according to the 'EIB's E&S standards, including potential disbursement conditions.[84]

3.1.2. Legal Framework

The principal law on identity management is the National Identity Management Commission Act. The law empowers the NIMC to manage the nation's identity program and establish a national identity database.[85] In addition, the law imposes the obligation to register and issue identity cards.[86] In fulfilling its mandate, the NIMC is expected to ensure the security and privacy of the database. Furthermore, the law makes it mandatory to use the National Identity Number.[87] In addition to the establishing Act, the NIMC has also issued secondary legislation to fulfil its statutory mandate. The NIMC has since issued the Mandatory Use of National Identification Number Regulation 2015, Regulations on the Mandatory Use of the National Identification Number, Nigeria Biometric Standards and other policy documents.[88]

3.2: Surveillance

---

[82] National Identification Commission of Nigeria (12 September 2018): "A Strategic Roadmap for Developing Digital Identification in Nigeria" HYPERLINK "http://citizenshiprightsafrica.org/a-strategic-roadmap-for-developing-digital-identification-in-nigeria

[83]/" http://citizenshiprightsafrica.org/a-strategic-roadmap-for-developing-digital-identification-in-nigeria/ accessed on 18 August 2021

ps://www.eib.org/en/projects/pipelines/all/20180298, accessed 26 August 2021

[84] Environmental and Social Data Sheet "Nigeria Digital ID", pg 3

https://www.eib.org/attachments/registers/84857112.pdf, accessed on 21 July 2021

[85] Section 14 of NIMC Act

[86] Section 18 NIMC Act

[87] Section 27 NIMC Act

[88] Policies (*National Identity Management Commission*2018) <https://nimc.gov.ng/policies/> accessed November 26, 2021.

Nigeria has a history of surveilling its citizens, a trend that appears to be a relic of previous military incursions into the politics and governance of the country.[89] While the 1999 Nigerian Constitution guarantees the right of Nigerians to privacy and freedom from interference,[90] the Nigerian State has been accused of consistently deploying a significant amount of resources towards the acquisition, installation and operation of high-tech surveillance equipment in contravention of this constitutional provision and standard international practices. [91]

3.2.1: The Legal and Regulatory Landscape

The legislation on surveillance was driven by national security and cybersecurity concerns.[92] Other legitimate aims advanced by the government is investigation and prevention of crime[93] in the interests of public emergency and safety and prevention of terrorism, which led to the enactment of the Terrorism Prevention Act. Frequent cyber-attacks were wreaking significant damage to consumers, foreign investments, and the perception of Nigeria in the comity of nation.[94] As a result, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 was passed by the National Assembly.

Another predominant legislation that serves as a legal basis for state surveillance is the Nigerian Communications Commission Act,[95] administered by the Nigerian Communications Commission (NCC). The law empowers the NCC to create and provide a regulatory framework for the Nigerian communications industry and other related matters. The law also aims to protect national interests and mandates all licensees to prevent crimes as far as reasonably necessary. The Commission reserves the discretion to determine if a licensee can implement the capability to allow the authorised interception of communications,[96] and can suspend licenses, take temporary control of services or networks; order the disclosure, interception or prevention of specified communications; or take possession of "network facilities,

[89] John Dada, Theresa Tafida: "Communications Surveillance in the Digital Age", Global Information Society Watch, https://giswatch.org/en/country-report/communications-surveillance/nigeria accessed on 17 July 2021

[90] Nigeria Communications Commission, Effects of Cybercrime of Foreign Direct Investment and National Development, pp. 93–94, https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file, accessed on 21 July 2021

[91] Al Jazeera (8 December 2020) "Nigerian intelligence bought tool to spy on citizens: Report" https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report

[92] Adeboye Adegoke: "Digital Rights and Privacy In Nigeria", Paradigm Initiative Publication Report, July 2020, pg 12

[93] Article 7.3 of Terrorism Prevention Act

[94] Nigeria Communications Commission, Effects of Cybercrime of Foreign Direct Investment and National Development, pp. 93–94, https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file

[95] Nigerian Communications Commission Act (2003 Act No. 19), LFN 2004

[96] Section 147 ibid

service, or customer equipment."[97] In furtherance of its mandate, the NCC has issued the following supplemental regulations, which comprise the legal regime for surveillance with significant privacy implications in Nigeria:

a. Guideline for Provision of Internet Service

Paragraph 6 of the Guidelines mandate ISPs to cooperate with 'all law enforcement and regulatory agencies investigating cybercrime or other illegal 'activity. In addition, ISPs must provide investigating authorities with service-related information, information about users, and the content of their communication. Paragraph 8 of the Guidelines mandate ISPs to retain user identification, message content, and traffic data for twelve months. The power to intercept communication data is not subject to judicial oversight.

b. The Registration of Telephone Subscribers Regulations, 2011[98]

The Regulations mandates licensees to capture subscriber information for retention in a central database established and maintained by the Commission and accessible to security agencies upon request by an official not below the rank of an Assistant Commissioner of Police or a coordinate rank in any other Agency.[99] However, the request to access these data is made to the NCC and not to a court of competent jurisdiction. A similar provision is retained in the proposed amendment to the Regulation.

c. The Nigerian Communications (Enforcement Process, etc.) Regulations, 2019[100]

The Regulations compels licensees to keep a record of call data according to the Cybercrimes Act and the Consumer Code Regulation and to avail the authorities with basic and non-basic information that may be required according to Section 146 of the Nigerian Communications Act.[101]

d. The Lawful Interception of Communication Regulations, 2019[102]

---

[97] Section 148 ibid

[98] Federal Republic of Nigeria Official Gazette, Consumer Code of Practice Regulations, 2007, https://www.ncc.gov.ng/docman-main/legalregulatory/regulations/102-consumer-code-of-practice-regulations-1/file, accessed on 30 July 2021

[99] Regulation 8, ibid

[100] Federal Republic of Nigeria Official Gazette, Nigerian Communications (Enforcement Process, etc.) Regulations, 2019, https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/840-enforcement-processes-regulations-1/file, accessed 22 August 2021

[101] Regulation 8 ibid

[102] Federal Republic of Nigeria Official Gazette, Lawful Interception of Communication Regulations, 2019, 23 Jan 2019, https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file, accessed 22 August 2021

The Regulation outlines the criteria under which communications may be intercepted, collected and shared in Nigeria. It criminalises the unauthorised interception of communication and allows interception by the Department of State Security, the Nigerian Police Force, and the National Security Advisor Office subject to a court warrant. However, there are instances where the surveillance can be conducted without the supervision of the court. Article 9 gives the authorised agencies the power to request protected or encrypted communications. Article 10 mandates service providers to install interception capabilities that permit interception, which impacts the integrity of communications. While the Regulation contains some safeguards, there are also clear safeguards omitted, which violate international human rights norms. For example, there is no obligation on law enforcement agencies to publish their transparency report publicly, notify individuals that are subject of interception to contest it, among other things.[103]

e. Federal Mutual Assistance Act 2019

This law aims to obtain and proffer mutual assistance in the prosecution of crimes on an international level. However, it impliedly allows the government to surveil Nigerian citizens on behalf of other countries to pursue criminals, investigate crimes, and share intelligence.

f. Terrorism Prevention Act 2011[104]

The Act authorises the Attorney General of the Federation or National Security Adviser to issue directives to any communications service provider to prevent, detect, or prosecute crimes.[105] Section 29 of the act empowers the relevant law enforcement agency to conduct intelligence gathering 'for the prevention of terrorist acts or to enhance the detection of offences related to the preparation of a terrorist act or the prosecution of offenders under this Act.'' The 'judge's order can permit the installation of a device to intercept communication, contrary to the principle of the integrity of communications.

g. Cybercrimes Act 2015

Section 45(2) (e) and (f) permit law enforcement officers to apply to a judge ex parte for a warrant to 'search any data contained in or available to any computer system or computer 'network' and to 'use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible

[103] Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059

[104] Federal Republic of Nigeria Official Gazette, Terrorism Prevention Act 2011 https://gazettes.africa/archive/ng/2011/ng-government-gazette-dated-2011-06-10-no-59.pdf, accessed 22 August 2021

[105] Section 26 ibid

'format'. Similarly, section 38(1) of the act mandates service providers to retain traffic and content data for two years. Further, section 38(2) of the act allows law enforcement agents to request data from service providers, and they are mandated to comply.

3.3: Encryption & Anonymity

In Nigeria, operators are expected to adhere to international standards concerning encryption and related issues.[106] On Tuesday, the 29th of June 2021, the commencement of National Key Infrastructure was initiated by the NITDA to provide security against unauthorised access and disclosure of stored information and ensure secure communication for all online services by addressing the fundamental elements of cybersecurity – confidentiality, integrity, authentication, and non-repudiation.[107]

3.3.1: The Legal & Regulatory Framework

a. Nigerian Data Protection Regulation 2019

In furtherance of the principle of security,[108] the NDPR mandates the development of "security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specifically authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of e-mailing systems and continuous capacity building for staff".[109]

b. Cybercrimes Act (Prohibition, Prevention Act) 2015

The law permits law enforcement personnel to "use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format after obtaining a warrant from a judge, subject to obtaining a warrant from the court.[110]Similarly, section 38(1) of the Act mandates service providers to retain traffic and content data for two years. Further, section 38(2) of the act allows law enforcement agents to request data from service providers, and they are mandated to comply.

---

[106] Rotimi Akapo and Oladotun Arokolaro (5 October 2018): "Telecoms Privacy and Data Security Provisions in Nigeria" 2018, https://www.lexology.com/library/detail.aspx?g=85f516e9-6520-4cf6-9c45-8ade7a2b70a5, accessed on 20 August 2021

[107] Ayoni M. Agbabiaka (30 June 2021): "NITDA introduces the Nigerian National Public Key Infrastructure https://www.blueprint.ng/nitda-introduces-the-nigerian-national-public-key-infrastructure/", accessed on 27 July 2021

[108] Article 2(1)(d) of the Nigerian Data Protection Regulation 2019

[109] Article 2.6 ibid

[110] See Section 45 of the Cyber Crimes (Prevention, Prohibition) Act 2015

c. Lawful Interception of Communications Regulation 2019

The law mandates licensees to, upon request, provide the relevant authorised Agency with the key, code, or access to the protected or encrypted communication, where the communication intercepted is encrypted or protected in the custody of the licensee.[111]

d. Registration of Service Telephone Subscribers Regulations 2011

The Regulation makes it mandatory to register SIM cards with biometric information.

e. Nigerian Communications (Enforcement Process, etc.) Regulations 2019

Regulation 8(1) prescribes that 'every licensee shall keep call data records under the Cybercrimes Act and the consumer code of practice 'regulations'.

f. Guideline for the Provision of Internet Service 2013

Paragraph 8 of the Guidelines mandate ISPs to retain user identification, message content, and traffic data for twelve months.

3.4: Cybercrimes and Cybersecurity: Data Breach and Violations

The 2020 Sophos Group survey revealed that 86% of 65 Nigerian companies which participated in the survey fell prey to cyberattacks within the past year.[112] According to the report, Nigeria had the highest percentage per sample size of data leakages worldwide and ranked top five for other forms of attacks, including ransomware, malware and cryptojacking. In October 2018, it was discovered that thousands of customers flying Arik Air, one of Nigeria's major airlines, may have had their data compromised in a major data leak.[113]

The Cybercrimes Act creates a comprehensive legal, regulatory, and institutional framework to prohibit, preempt, detect, prosecute, and punish cyber offences in Nigeria.[114] It also encourages the protection of important critical national infrastructure and the security of computer systems, networks and programs,

[111] See Regulation 9 of the Lawful Interception of Communications Regulation 2019

[112] ibid pg 21

[113] Oladeinde Olawoyin (31 Oct 2018): Massive Data Leak Affecting Arik Air Customers; Company Slow to Respond: Paine, Data Breaches, https://www.databreaches.net/massive-data-leak-affecting-arik-air-customers-company-slow-to-respond-paine/

[114] Josephine Uba (7 July 2021): "Cybercrimes And Cyber Laws In Nigeria: All You Need To Know", https://www.mondaq.com/nigeria/security/1088292/cybercrimes-and-cyber-laws-in-nigeria-all-you-need-to-know accessed on 22 August 2021

intellectual property, and privacy rights. It establishes the Cybercrimes Advisory Council ("CAC")[115] and saddles it with the responsibility for formulating and providing general policy guidelines for preventing and combating cybercrimes and the promotion of cybersecurity in Nigeria. The office of the National Security Adviser serves as the coordinating authority for all other security and enforcement bodies. The Economic and Financial Crime Commission Act, 2004[116] also provides a legal framework for investigating all financial crimes, including advance fee fraud, money laundering, charge transfers, fraudulent encashment of negotiable instruments, computer credit card fraud and contract scams among others. In 2014, Nigeria adopted a National Cybersecurity Strategy and Policy. The Strategy was revised and released in February 2021.[117]

The Nigeria Computer Emergency Response Team ("ngCERT"), domiciled in the office of the National Security Adviser, is the National Computer Emergency Response Team for Nigeria and is tasked with achieving "a safe, secure and resilient cyberspace in Nigeria that provides opportunities for national prosperity".[118] The team carries out proactive services (like intrusion detection services, vulnerability assessment and penetration testing, and technology watch), reactive services (like alerts and warnings, incident handling, forensic analysis and vulnerability handling) and security quality management services. The Council also maintains a portal for reporting vulnerabilities and incidents integrated into the 'Council's official website. NgCERT operates to prepare, protect, and secure Nigerian cyberspace in anticipation of attacks, problems, or events and reduce the volume of future incidents.[119]

In contrast with the numbers highlighted in the survey, the regulators' administrative fines and punitive measures in response to these breaches appear inadequate. Data Controllers have a duty of self-reporting personal data breaches to NITDA within 72 hours of knowledge of such breach.[120] The Data Controller is also required to immediately notify the Data Subject of the personal data breach where the personal data breach will likely result in high risks to the freedoms and rights of the data subject.[121] The NDPR addresses several issues related to data management, one of which is the governing principles of data processing. It foists

[115] Section 42 of the Cybercrimes Act 2015, ibid

[116] The Economic and Financial Crime Commission (Establishment) Act, Cap E1, LFN 2004

[117] Nigeria Launches National Cybersecurity Policy and Strategy <https://www.wadr.org/news.php?uin=WN2502215581> accessed November 26, 2021.

[118]

[119] The Council's official website can be accessed via https://www.cert.gov.ng/.

[120] Paragraph 9.2 of the NDPR Implementation Framework 2019

[121] Paragraph 9.4 ibid

an obligation on data controllers to ensure that personal data is secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by fire or rain, or exposure to other natural elements.[122]

Article 2.10 provides the penalty for breach for default under the NDPR. Where a data controller handling the data of more than 10,000 data subjects is in default, the fine will be a payment of 2% of the annual gross revenue of the preceding year or the sum of N10 million, whichever is greater. Where the Controller handles the personal data of less than 10,000 data subjects, the fine will be 1% of the annual gross revenue of the preceding year or the sum of N1 million, whichever is greater. The foregoing is exclusive of any criminal liability that the defaulter may additionally attract in law.

NITDA also issued the Guidelines for the Management of Personal Data by Public Institutions in Nigeria (the Guidelines) 2020. It is meant to serve as an implementation framework for public institutions concerning the NDPR. One of its requirements for public institutions is to appoint a Data Protection Officer (D.P.O.). This DPO will carry out several duties, one of which is to advise management on practices that could trigger breaches under Article 2.6.b.vi. The Guidelines further provide that sharing databases via mail, hard copies, files, or any other format not in conformity with the defined format will be a breach, under 4.0.c. For the sake of context, the approved format under 4.0.b is by way of encryption or any other cryptographic method that prevents personal data from being accessed by unauthorised third parties. Article 7.0b further provides that principal officers of public institutions can be held personally liable for misuse of personal information shared, both while they were in office and after.

Other laws provide the requirement to notify regulators or data subjects about data breaches. Section 21 of the Cybercrimes Act creates the obligation for organisations to report data breaches to the Nigeria Computer Emergency Team (ngCERT). This must be done immediately after the attack occurs. Failure to report after seven days of the incident is punishable with denial of internet service and a fine of 2 Million Naira ($6,535). Article 4.3 of the Nigeria Communications Commission Internet Code of Practice provides that an Internet Access Service Provider shall notify affected customers of any breach relating to the 'customer's information within 48 hours of its occurrence, by e-mail and text message. In addition, an Internet Access Service Provider shall formally notify the Commission in writing of any breach no later than 48 hours after the Internet Access Service

[122] See Article 2(1)(d) of the Nigerian Data Protection Regulation 2019

Provider reasonably determines that a breach has occurred. Section 5.2 of Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers prescribes that " a DMB/PSP is required to report all cyber-incidents whether successful or unsuccessful not later than 24 hours after such incident is detected to the Director of Banking Supervision, Central Bank of Nigeria".

4.0
Major Events on each Thematic Areas

4.1: Data Protection Enforcement

The industry regulator, NITDA, has been relatively busy in this regard. In the 2019-2020 year of review, 230 compliance and enforcement notices were issued and served, 790 issues were resolved, 15 investigations were conducted into alleged data breaches, 7 data controllers were listed for immediate enforcements, and one investigation was concluded. For example, in December 2019, taxpayers' data in Lagos State were leaked from the Lagos Internal Revenue Service (LIRS) https://lagos.qpay.ng/TaxPayer, prompting NITDA to launch an investigation into LIRS. A fine of One Million Naira (₦ 1,000,000.00) was consequently imposed on the LIRS.[123] Also, a public advisory was issued on the Truecaller service, leading to the review and improvement of its privacy notice with the assistance of NITDA.[124]

On the 16th of March 2021, NITDA announced that it had imposed its second data breach fine of ₦ 5 million on Electronic Settlement Limited (ESL) for personal data breach following a 16-month investigative process.[125] On the 17th of August 2021, NITDA announced the imposition of a fine of N10 million on SokoLoans, an online lending platform, for collecting the contacts of defaulters and sending them disparaging messages about the defaulters.[126] NITDA has also announced plans to go after other lending platforms, including Palmcredit and 9credit, for similar practices as SokoLoans.[127]

[123] Yinka Okeowo (10 October 2020): "NITDA Fines LIRS N1million for Alleged Breach of Data Protection Regulation" https://techeconomy.ng/2020/10/nitda-fines-lirs-n1million-for-alleged-breach-of-data-protection-regulation/, accessed on 26 August 2021

[124] Techeconomy (23 September 2019) Truecaller under investigation by NITDA over a potential breach of privacy rights of Nigerians https://techeconomy.ng/2019/09/truecaller-under-investigation-by-nitda-over-potential-breach-of-privacy-rights-of-nigerians/,

[125] Andersen Tax (9 April 2019): "NITDA Fines Company for Data Breach; Extends Filing Deadline to 30th June 2021, https://ng.andersen.com/nitda-fines-company-for-data-breach-extends-filing-deadline-to-30th-june-2021/, accessed on 26 August 2021

[126] One Trust Data Guidance (18 August 2021): Nigeria: NITDA issues first NDPR fine of NGN 10M against SokoLoan https://www.dataguidance.com/news/nigeria-nitda-issues-first-ndpr-fine-ngn-10m-against

[127] Olalekan Fakoyejo (19 August 2021), 'Government Agency to Go After 9Credit, Palmcredit as SokoLoan tried to avoid N10 million fine', (Legit, August 19, 2021) https://www.legit.ng/1430228-government-agency-go-after-9credit-palmcredit-soko-loan-tries-avoid-n10million-fine.html accessed on 27 august 2021

4.2: Digital and Biometric Identity

Various events and trends have characterised Nigeria's digital and biometric identity landscape. For example, in 2007, when the National Identity Management Commission (NIMC) kicked off the national database identification project, the Commission received funding of 30 billion Naira to collect data and operate a turnkey infrastructure created by SAGEM a French telecommunications company. The government agreed to pay SAGEM about $216 million for offshore components and 2 billion Naira for onshore components intended to be managed by NIMC. However, the enrollment did not begin until 2013, and the foreign company contracted for the project has refused to hand over the turnkey system to NIMC, claiming it is due to a payment of $6.1 million maintenance fees inclusive of the $2.444 million for 8 million cards it has not delivered. Unfortunately, SAGEM currently has a database of over 52 million Nigerians.[128]

Interestingly, in 2009, the National Identity Management Commission (NIMC), in implementing the National Identity Management Systems (NIMS) for Nigeria, commissioned contracts for conducting Privacy Impact Assessment (PIA) studies to identify the potential effects that the proposed system may have upon personal privacy; and to examine how any such detrimental effects on privacy might be reduced.[129] Findings from the assessment revealed that over 90 per cent of Nigerians welcomed the project and were ready to participate in it. The report also noted that 83.4 per cent of respondents had no fears of infringement on their privacy.[130]

On the 4th of April 2017, the NIMC renewed its contract with Safran Identity & Security to upgrade its existing automatic biometric identification system (ABIS) to the new MorphoBSS (Morpho Biometric Search Services) using three types of biometrics: face, iris and fingerprints. This system will enable the NIMC to create a reliable identity database of citizens and residents of Nigeria, and each person will be identified by a unique National Identification Number (NIN).[131] In the same year, the National Population Commission commissioned Bio-Metrica's Multi-Factor

[128] 'Nigeria's Poor Data Culture' (iAfrikan.com, 10 August 2020) <https://iafrikan.com/2020/08/10/nigeria-and-its-poor-data-culture/> accessed 23 November 2021

[129] National Identity Management Commission 'Privacy Impact Assessment Report' <https://nimc.gov.ng/docs/pia_report.pdf> accessed 23 November 2021

[130] 'Nigerians embrace National ID infrastructure upgrade' (Vanguard 17 June 2009) <https://www.vanguardngr.com/2009/06/nigerians-embrace-national-id-infrastructure-upgrade/> accessed 23 November 2021

[131] 'Nigeria Retains Safran Identity & Security to Provide an Upgraded Automatic Biometric Identification System and Maintenance Support' (IDEMIA) <https://www.idemia.com/press-release/nigeria-retains-safran-identity-security-provide-upgraded-automatic-biometric-identification-system-and-maintenance-support-2017-04-04> accessed 23 November 2021

Biometric Census Registration System (CRS) for the 2018 Population Census. This system will use biometrics to ensure all citizens are properly identified and reduce fraud by collecting their fingerprints and facial biometrics.[132] Similarly, at the Nigeria Electronic Fraud Forum, in 2017, the Central Bank of Nigeria (CBN) announced plans to replace PINs with biometric scans at ATMs.[133]

Low public awareness, little public consultation, and agencies performing overlapping functions are also factors that characterise the landscape.[134] About 17 federal and state agencies currently offer and regulate ID services in Nigeria, with many collecting the same data from the same individuals. Although efforts have been made to harmonise the framework as far back as 2014, this is yet to be achieved. The initial roll-out of the 'eID' card, which was undertaken in partnership with MasterCard, was heavily criticised as a profit-motivated venture that branded citizen data, given 'MasterCard's ties to major financial institutions in the United States.[135] In a 2017 exchange, a Twitter user, Tọ̀míwá Ilọ̀rí, questioned the 'NIMC's claims of ownership of the data of Nigerians.[136] On its official website and Twitter bio, the Agency claims to have the mandate to "establish, own, operate, maintain and manage the National Identity Database in Nigeria" in exercising powers beyond those contemplated in the NIMC Act.

Furthermore, at the meeting of the Federal Executive Council on the 12th of September, 2018, chaired by President Muhammadu Buhari, the President approved the new National Digital Identity Ecosystem Strategic Roadmap for the enrolment of Nigerians and legal residents into the National Identity Database (NIDB) and mandated the use of the National Identification Number (NIN), from the 1st of January, 2019.[137] This drew the ire of concerned stakeholders, with Paradigm Initiative calling for the immediate suspension of the scheme due to concerns over the 'NIMC's ability to ensure the protection of the mass citizen data in their possession, a risk heightened by the absence of a substantive and comprehensive

[132] 'Nigerian Authorities to Register Citizens' Biometrics in 2018 Census' (FindBiometrics, 23 January 2017) <https://findbiometrics.com/nigerian-biometrics-census-401233/> accessed 23 November 2021

[133] 'Central Bank of Nigeria Plans for Biometric ATMs' (FindBiometrics, 20 November 2017) <https://findbiometrics.com/central-bank-nigeria-biometric-atms-411203/> accessed 23 November 2021

[134] The Engine Room (January 2020): "Understanding the Lived Effects of Digital ID A Multi-Country Study, Annex D, Digital ID In Nigeria: A Case Study", pp 112 – 128

[135] O'Grady, S. (2014, September 3) Nigeria's Orwellian Biometric ID Is Brought to You by MasterCard https://foreignpolicy.com/2014/09/03/nigerias-orwellian-biometric-id-is-brought-to-you-by-mastercard/, accessed on 30 July 2021

[136] Tomiwa Ilori (16 May 2017): "You don't own Nigerians' data," https://twitter.com/tomiwa_ilori/status/864445561835048963, accessed 27 July 2021.

[137] Yinka Okeowo (January 1, 2019): National Identity Number has become mandatory from today – NIMC https://techeconomy.ng/2019/01/national-identity-number-has-become-mandatory-from-today-nimc/, accessed on 17 July 2021

Nigerian data protection law.[138] Subsequent investigations later revealed that the codes provided for people to access their NINs lacked critical security protocols and were prone to breach by cybercriminals.[139]
Among other issues cited were low levels of public awareness, little or no public consultations, lack of informed consent and data protection concerns.[140] Nevertheless, despite the slow start of the scheme, NIMC claims to have recorded more than 60 million unique NIN records in the National Identity Database (NIDB) as of the 29th of July, 2021.[141]

The NIMC, which is now supervised by the Federal Ministry of Communications and Digital Economy,[142] is also championing an Africa-first Mobile Identity Ecosystem by leveraging the Open Standards Identity APIs (OSIA) framework to authenticate NINs by matching them to the national identity registry.[143] OSIA is an accessible standard set of interfaces developed to enable smooth connectivity between all parts of the identity management ecosystem and prevent vendor lock-in. As part of the initiative, the NIMC Mobile ID Ecosystem allows citizens to verify their ID against the National Identity Registry quickly and securely with biometrics via an OSIA interface.

In 2020, Nigeria deployed Integrated Biometrics (IB) Scanners to register customers for its Nigeria Inter-Bank Settlement System (NIBSS) and to link each individual to a unique Bank Verification Number (BVN). According to the Central Bank of Nigeria, the introduction of Integrated Biometrics (IB) Scanners provides the NIBSS with a way to link each individual to their BVN, without traditional methods like PINs and passwords that are not strong enough to prevent fraud.[144] However, in August of the same year, the NIMC leaked the personal data of some Nigerians through its NIMC App meant for processing digital national identity cards. Following this, a Non-governmental organisation, the Laws and Rights Awareness Initiative,

[138] Yinka Okeowo (January 9, 2019) Reasons Paradigm Initiative wants NIMC to suspend NIN enforcement activities https://techeconomy.ng/2019/01/reasons-paradigm-initiative-wants-nimc-to-suspend-nin-enforcement-activities/, accessed on 30 July 2021

[139] Adeboye Adegoke supra, pg 7

[140] Ibid

[141] NIMC News (29 July 2021): "NIMC Reaches More than Sixty (60) Million Unique NIN Records" https://nimc.gov.ng/nimc-reaches-more-than-sixty-million-60-unique-nin-records/

[142] Chika Oliseh, August 31, 2020: Buhari approves transfer of NIMC to Federal Ministry of Communications and Digital Economy https://nairametrics.com/2020/08/31/buhari-approves-transfer-of-nimc-to-federal-ministry-of-communications-and-digital-economy/

[143] Ayang Macdonald (13 May 2021): "Nigeria reiterates crucial role of biometric national ID, updates SIM registration policy", https://www.biometricupdate.com/202105/nigeria-reiterates-crucial-role-of-biometric-national-id-updates-sim-registration-policy accessed 29 August 2021

[144] 'Nigeria Uses Integrated Biometrics Scanners to Power Bank Identification System' (FindBiometrics, 9 February 2021) <https://findbiometrics.com/nigeria-uses-integrated-biometrics-scanners-power-bank-identification-system-020907/> accessed 23 November 2021

instituted an action before the Federal High Court against the Commission for data breach and omission to conduct data protection impact assessment.[145]

In June 2021, Spanish identity provider 'FacePhi' was introduced into the Nigerian Armed Forces. 'FacePhi' is a biometric system that helps people to access banking and financial services. It was introduced into Nigeria to help facilitate the distribution of pension benefits to veterans and retired military personnel. The system is operatable from the users' smartphones remotely. It first asks veterans to take a photo of an official ID card and analyses the characters on the surface to ensure the card is authentic. After that, users will need to take a selfie which the system will match with the image on the ID. [146] In addition, some state governments have also adopted biometric residential registration schemes[147], and the biometric capturing has also been extended to prisons[148], vulnerable populations in Internal Displaced Persons Camps[149] and school children[150] in different parts of the country. This has also been adopted for the verification of civil servants[151] .

[145]Chioma U, 'National Digital Identity Card: NGO Seeks Injunction Against NIMC For Data Breach And Omission To Conduct Data Protection Impact Assessment' (TheNigeriaLawyer, 17 August 2020) <https://thenigerialawyer.com/national-digital-identity-card-ngo-seeks-injunction-against-nimc-for-data-breach-and-omission-to-conduct-data-protection-impact-assessment/> accessed 23 November 2021

[146] 'Nigerian Military Turns to FacePhi to Distribute Pension Benefits' (FindBiometrics, 25 June 2021) <https://findbiometrics.com/nigerian-military-turns-facephi-distribute-pension-benefits-062508/> accessed 23 November 2021

[147] Oyo Commences Residents' Registration Monday (*Tribune Online*August 6, 2021) <https://tribuneonlineng.com/oyo-commences-residents-registration-monday/> accessed November 26, 2021.

4 Million Residents Register with LASRRA | the Guardian Nigeria News - Nigeria and World News https://guardian.ng/news/4-million-residents-register-with-lasrra/> accessed November 26, 2021.

[148] Nigeria Counts on Biometrics to Recapture Nearly 4K Fleeing Jail-Breakers | Biometric Update <https://www.biometricupdate.com/202111/nigeria-counts-on-biometrics-to-recapture-nearly-4k-fleeing-jail-breakers> accessed November 26, 2021.

[149] Digital Identity for Nigerian Internally Displaced Persons Approved by Government | Biometric Update <https://www.biometricupdate.com/202011/digital-identity-for-nigerian-internally-displaced-persons-approved-by-government> accessed November 26, 2021.

[150] Nigeria Collects Biometrics of Elementary School Children for Meal Program | Biometric Update <https://www.biometricupdate.com/202110/nigeria-collects-biometrics-of-elementary-school-children-for-meal-program> accessed November 26, 2021.

[151] Nigerian Government Begins Biometric Verification Pilot for Civil Servants | Biometric Update <https://www.biometricupdate.com/201506/nigerian-government-begins-biometric-verification-pilot-for-civil-servants> accessed November 26, 2021.

Also, in 2020, the NIMC licensed some private organisations as capturing agents to assist with registration and verification service providers.[152] It is instructive to know that the eligibility criteria did not include evidence of implementation of data protection and cybersecurity measures.[153]Also, it is not publicly available if NIMC demanded assurance in this regard or conducted a vendor verification exercise from a security and data protection standpoint or safeguard for data-sharing arrangement. Finally, there is no public record to demonstrate that the NIMC conducted a data protection impact assessment or a human rights impact assessment before commencing the identity program. It is uncertain if Nigeria's identity program will suffer the same fate as Kenya, where a court ruled that the government identity program is invalid for failure to comply with the Kenyan Data Protection Act and was asked to conduct a data protection impact assessment.[154]

4.3 Surveillance

Nigeria has a long history of surveillance at the federal and state levels of government. In 2013, the investigative journalism newspaper, Premium Times, reported that the Goodluck Jonathan administration contracted and opaquely awarded $40 million to Elbit Systems, an Israeli firm, in breach of due process and public procurement protocols. Elbit was allegedly contracted to supply technology that enables the state to intercept all internet activity and invade users' privacy at will.[155] In a report published by the University of 'Toronto's Citizen Lab, 'Nigeria's Defence Intelligence Agency was alleged to have acquired equipment that it can use to spy on its 'citizens' calls and text messages.[156] The report further indicated a telecom surveillance company called "Circles" that has allegedly been helping state security apparatuses across 25 countries, including Nigeria, spy on the communications of opposition figures, journalists, and protesters.[157] The company

---

[152] 'Public Notice: Approved Data Capturing Agents (Digital Identity Ecosystem)' (*National Identity Management Commission*) <https://nimc.gov.ng/public-notice-approved-data-capturing-agents-digital-identity-ecosystem/> accessed 22 October 2021.

[153] "Federal Ministry of Communications and Digital Economy NATIONAL IDENTITY MANAGEMENT COMMISSION ELIGIBILITY CRITERIA for SELECTION of SERVICE PROVIDER FOR" <https://nimc.gov.ng/docs/reports/eligibility_criteria_verification_services.pdf> accessed October 22, 2021.

[154] 'Kenya: Courts Declare Huduma Namba Invalid : Citizenship Rights in Africa Initiative' <https://citizenshiprightsafrica.org/kenya-courts-declare-huduma-namba-invalid/#:~:text=The%20High%20Court%20has%20declared,the%20Constitution%20in%20the%20process.> accessed 22 October 2021.

[155] Ogala Emmanuel, Exclusive: Jonathan Awards $40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians, Premium Times, 25 April 2013, https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-toisraeli-company-to-monitor-computer-internet-communication-by-nigerians.html, accessed 20 July 2021

[156] Al Jazeera News (8 December 2020) Nigerian intelligence bought tools to spy on citizens: Report https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report, accessed 25 July 2021

[157] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," Citizen Lab Research Report No.133, University of Toronto, December 2020, p9.

allegedly sells high-tech systems to exploit the vulnerabilities of Signalling System 7 (SS7), which allows one mobile network to connect with another. According to Premium Times, 2 Nigerian Governors have allegedly acquired and deployed this spyware.[158]

Expenditure on surveillance equipment also appears in the national budget and records of public expenditure. The Nigerian government spent at least 127 million USD on surveillance and security equipment between 2014 and 2017. Peculiar expenses such as the "Stravinsky Project" and the "All- Eye" surveillance project were also part of the budgetary allocations for the Office of the National Security Adviser and Department of State Services in the 2020 budget. In 2020 alone, the government is reported to have earmarked five billion Naira on surveillance-related technologies.[159] The Director of Defence Information, Major-General John Enenche, was publicly quoted to have admitted that certain "strategic media centres" have been designated to monitor social media.[160] The Committee to Protect Journalists reported that the Nigerian military has used digital forensic technologies to extract information from phones and computers to spy on ordinary Nigerians and the press.[161]

The Nigerian Senate in July 2021 approved 4.8 billion Naira (US$11 million) to the Nigerian Intelligence Agency for the purchase of WhatsApp Intercept Solution and Thuraya Interception Solution, 'a communications system used for monitoring voice calls, call-related information, short message service (SMS) and data traffic, among 'others'. The deployment of these tools will impact end-to-end encryption for 'communication'.[162] A decision currently being challenged at the Federal High Court by an advocacy group for violation of the constitutionally guaranteed rights to freedom of expression and privacy.[163]

---

[158] ibid p10

[159] Adeboye Adegoke supra, pg

[160] O. Ayodele, (23 Aug 2017), "Military Monitoring Social Media for Hate Speech", https://punchng.com/military-monitoring-social-media-for-hate-speech-enenche/ accessed on 30 July 2021

[161] Jonathan Rozen 22 October 2019), "Nigerian Military Targeted Journalists' Phones, Computers with "Forensic Search" for Sources, Committee to Protect Journalists", https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/ accessed on 30 July 2021.

[162] 'Nigerian Govt Moves to Control Media, Allocates N4.8bn to Monitor WhatsApp, Phone Calls' (12 July 2021) <https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html> accessed 22 October 2021.

[163] 'SERAP Drags Buhari to Court over Plan to Monitor WhatsApp Calls, Messages' (*Vanguard News*, 17 October 2021) <https://www.vanguardngr.com/2021/10/serap-drags-buhari-to-court-over-plan-to-monitor-whatsapp-calls-messages/> accessed 22 October 2021; See also 'No to Monitoring of Nigerian's Communications' (Punch Newspapers, 19 October 2021) <https://punchng.com/no-to-monitoring-of-nigerians-communications/> accessed 23 November 2021

Furthermore, the laws enabling surveillance in Nigeria do not meet the threshold established under the International Principles on the Application of Human Rights to Communications Surveillance and the Declaration of Principles on Freedom of Expression and Access to Information in Africa. Principle 41 of the African Declaration stipulates that,

Any law authorising interference through surveillance regimes shall provide for:

a. the prior authorisation of an independent and impartial judicial authority;
b. due process safeguards;
c. specific limitation on the time, manner, place and scope of the surveillance;
d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
e. proactive transparency on the nature and scope of its use; and
f. effective monitoring and regular review by an independent oversight mechanism.

However, not all surveillance activity is approved by a judge, under the Registration of Telecommunication Subscribers Regulations, the NCC and not a court grants investigating authorities access to subscribers' data. Similarly, the investigating authorities do not make public records of surveillance conducted or inform the individuals subject to surveillance after the act. Furthermore, the Nigerian surveillance legal framework does not provide for an independent oversight body. The laws are spread across different documents, and they do not make surveillance necessary only for serious crimes, as it is being used for trivial offences. The investigating authorities also do not conduct a human rights impact assessment before deploying these tools. Finally, it is difficult to know which law is being relied upon because of the lack of transparency, which has led to the abuse of these powers to target journalists and even opposition members.[164] The obvious lack of sufficient safeguards is contrary to the international human rights principles on communications surveillance.

4.4 Cybercrime and Cybersecurity

Due to increasing and severe incidents of cybercrimes, cybercrimes against people include cyber harassment and stalking, e-mail phishing, identity theft, credit card fraud, the dissemination of child pornography, various sorts of spoofing, human trafficking, and online connected libel or slander; the Nigerian government has shone a spotlight on cybercrime and cybersecurity for many years now through the

[164] 'Investigation: How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others | Premium Times Nigeria' (9 June 2016) <https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html> accessed 22 October 2021.

Economic and Financial Crime Commission (EFCC), which acts as the government watchdog for this purpose.

The results of a global survey[165] carried by Sophos, a global leader in next-generation cybersecurity, revealed that about 51% of organisations experienced a significant ransomware attack in the previous 12 months, compared to 54% in 2017.[166] In Nigeria, 53 per cent of the organisations that participated in the survey admitted to being the target of at least one ransomware attack within the past year. Globally, data was encrypted in about 73% of attacks that successful attacks.[167] In Nigeria, it was 74%. In addition, more than 27% of organisations hit by ransomware admitted to paying the ransom demanded by the attackers. The survey also revealed that 38% of the Nigerian organisations that were subjects of attacks admitted paying the ransom.[168]

According to the Nigerian Electronic Fraud Forum (NEFF), commercial banks in Nigeria were reported to have lost an aggregate sum of N15 billion (US$39 million) to cybercrime and electronic fraud in 2018 alone, a staggering 537% increase on the N2.37 billion loss recorded in 2017[169]. In addition, fraud rose by 55% from the previous year, and more than 17,600 bank customers and depositors lost N1.9 billion to cyber fraud in 2018.[170] These losses are forcing Nigerian lenders to commit more resources into cybersecurity, even if losses are expected to grow as more Nigerians adopt digital banking solutions. According to Nigeria's Consumer Awareness and Financial Enlightenment Initiative, as much as US$6 trillion may be lost to the activities of cybercriminals in and out of Nigeria within the next ten years.[171]

A gang of hackers reportedly made away with N900 million (US$24 000) from a top commercial Nigerian bank using sophisticated malware in Lagos in 2018. According to the EFCC, the hackers eventually mirrored bank employee workflows by covertly installing spying software on bank computers and illegally transferring transfers into bank accounts they had created for the heist.[172]

---

[165] Sophos Group Report supra, p3

[166] id pg5

[167] id pg 6

[168] id pg 9

[169] Zolonye Ushedo Apr 8, 2021: "How thieves use Covid-19 to defraud bank accounts" https://nairametrics.com/2020/05/12/how-thieves-use-covid-19-to-defraud-bank-accounts/ accessed on Jul 27, 2021

[170] Ibid

[171] Collins Nweze (The Nation): CAFEi predicts $6tr global loss to cybersecurity https://thenationonlineng.net/cafei-predicts-6tr-global-loss-to-cybersecurity/ accessed on Jul 28, 2021

[172] Ya'u Mukhtar (7 May 2021): Cybercrimes in Nigeria and the Security Implication, https://prnigeria.com/2021/05/07/cybercrimes-nigeria-security-implication/, accessed on 30 august 2021

Also, public authorities have been subjects of cybersecurity attacks. Even though the Nigerian government, through the National Cybersecurity Strategy, has designated some sectors as Critical National Information Infrastructure, there are records of government websites being defaced, in 2015, of the "2,175 websites that had been defaced, 585 were government websites".[173] In 2018, 80,000 Nigerians who were part of the national HIV/AIDS survey data suffered a breach.[174]During the national election in 2015, the website of the national electoral body got hacked.[175]In 2020, the NIMC was engrossed in a debacle over the unauthorised access to the National Identity Number (NIN) of people through its mobile application, available publicly for download on a popular mobile application store.[176] In addition, there is a growing distrust for the government over the handling of citizens personal data.

4.5 Multiple Mandatory Government Registration

The Nigerian government has created multiple mandatory biometric registrations for citizens and residents at federal and state levels. In some instances, a mandatory identity is required to access public services. There have been concerns by civil society and citizens alike over the privacy and security of their information in the hand of public authorities. Lagos State government issues resident cards.[177] Similarly, Oyo[178] and Kaduna[179] have also mooted the idea. The state government have often cited insecurity as the reason for registering residents. "Multiple state agencies now require a fingerprint, facial capturing or other biometric data for

[173] 'NSA, Microsoft Team up to Tackle Cybercrime in Nigeria' (*Vanguard News*, 2 December 2015) <https://www.vanguardngr.com/2015/12/nsa-microsoft-team-up-to-tackle-cybercrime-in-nigeria-2/> accessed 22 October 2021.

[174] '80,000 Nigerians Medical Data at Risk After Worldwide Leak' (22 September 2020) <https://web.archive.org/web/20200922050435/https://www.cybersecfill.com/80000-nigerians-medical-data-at-risk/amp/> accessed 22 October 2021.

[175] 'The Independent Nigerian Electoral Commission's Website Has Been Hijacked' (*TechCabal*, 28 March 2015) <https://techcabal.com/2015/03/28/nigerias-electoral-commissions-website-has-been-hijacked/> accessed 22 October 2021.

[176] Olugbenga ADANIKIN, 'NIN: How Presidential Aide Exposed Nigerians to Data Breach via NIMC Mobile App Registration' (*International Centre for Investigative Reporting*, 18 August 2020) <https://www.icirnigeria.org/nin-how-presidential-aide-exposed-nigerians-to-data-breach-via-nimc-mobile-app-registration/> accessed 22 October 2021.

[177] Lagos State Residents Registration Agency (*LASRRA*2020) <https://www.lagosresidents.gov.ng/> accessed October 22, 2021.

[178] 'Insecurity: Oyo to Register Residents' (*Peoples Gazette*, 23 June 2021) <https://gazettengr.com/insecurity-oyo-to-register-residents/> accessed 22 October 2021.

[179] 'Kaduna Mandates Use of Resident Card, NIN' (*Daily Trust*, 25 February 2021) <https://dailytrust.com/kaduna-mandates-use-of-resident-card-nin> accessed 22 October 2021.

identification. No less than six government agencies maintain different biometric data points on citizens and residents at the federal level".[180][181]

The multiple collections of biometric data by different government agencies have been a source of worry. Each government agency requests a similar data set to access basic services, and failure to register could cause a denial of service. In 2015, President Buhari directed data collection agencies to aggregate their databases.[182] However, citizens and legal residents still have to register with the respective agencies without interoperability. There is a mistrust by the public towards the government about the handling of their personal data.[183]

Subscriber Identification Modules (SIMs) are a necessary component for citizens to access various telecommunication services. However, the Nigerian government makes it mandatory to register SIM cards with the holders' biometric information.[184] The government reason for this is to curb insecurity. Generally, mandatory SIM card registration has been criticised for 'eradicat[ing] the anonymity of communications, enable[ing] location-tracking, and simplify[ing] communications surveillance and interception. Furthermore, facilitating the creation of an extensive database of user information places individuals at risk of being tracked or targeted and having their private information misused.[185] Nevertheless, SIM registration schemes threaten to throttle the technology's developmental potential, with serious privacy and other human rights violations.[186] Further to an audit carried out by the NCC, it was discovered that while over 53 million people are already registered NIN in the NIMC database, there were still 9.4 million allocated but improperly or unregistered SIM cards.[187]

---

[180] Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059

[181] Independent National Electoral Commission (voter card); Central Bank of Nigeria (bank verification number); Nigeria Police Force (tint permit, which allows drivers to wear tinted glasses); Federal Road Safety Commission (driver's licence); Nigeria Immigration Commission (international passport and residential permit); and National Identity Management Commission

[182] 'Data Collection Agencies Get Presidential Order to Aggregate Databases' (*National Identity Management Commission*) <https://nimc.gov.ng/data-collection-agencies-get-presidential-order-to-aggregate-databases/> accessed 22 October 2021.

[183] Got Your Number: Privacy Concerns Hobble Nigeria's Digital ID Push *Reuters* (5 August 2021) <https://www.reuters.com/article/nigeria-tech-rights-idUSL8N2OW2CJ> accessed 22 October 2021.

[184] Revised National Identity Policy for Sim Card Registration https://www.ncc.gov.ng/documents/988-revised-national-identity-policy-for-sim-card-registration/file accessed on 27 august 2021

[185] '101: SIM Card Registration' (*Privacy International*) <http://privacyinternational.org/explainer/2654/101-sim-card-registration> accessed 22 October 2021.

[186] Kevin Donovan and Aaron K. Martin, "The Rise of African SIM Registration: The emerging dynamics of regulatory change, First Monday, Volume 19, Number 2 - 3 February 2014 https://firstmonday.org/ojs/index.php/fm/article/download/4351/3820/38289 accessed on 27 august 2021

[187] Revised National Identity Policy for Sim Card Registration https://www.ncc.gov.ng/documents/988-revised-national-identity-policy-for-sim-card-registration/file accessed on 27 august 2021, pg 20

On the 15th of December, 2020, the Federal Government (FG), through the Minister of Communications and Digital Economy, Isa Pantami, directed all telecommunications operatives to disconnect all mobile telephone lines not linked to valid National Identification Numbers (NINs), with a 2-week compliance deadline for subscribers who were yet to synchronise their SIM cards. Telcos who failed to comply with the directive to block SIM cards not linked to their NINs might have their operational licenses suspended.[188] However, stakeholders raised concerns over privacy and data processing. In February 2020, a Civil rights group coalition Edo Civil Society Organisations (EDOCSO), sued at the Federal High Court in Edo state capital, Benin, praying the court to declare the move as a breach of citizens' right to privacy.[189] In May 2021, the NCC updated its identity policy to state that SIM card acquisition and activation should be made based on NIN verification using biometric methods such as facial recognition and fingerprints, which would be matched against data held by the NIMC.[190]

4.6 Anonymity and Encryption

The Cybercrimes Act and Lawful Interception Communication Regulations (LICR) provide the legal basis for the government to order the decryption of encrypted communications. Similarly, the Senate's approval of the supplementary budget to allow the National Intelligence Agency to acquire surveillance tools that will target WhatsApp, an end-to-end encrypted communication tool, is an affront to the freedom of expression and the right to privacy. Also, the provision of the LICR mandating the telecommunication company to install interception tools in their infrastructure weakens the integrity of communications. The admission by security agencies to procuring surveillance tools capable of assisting the government with decryption of encrypted data also suggests that the Nigerian government is complicit in carrying out anti-encryption policies.[191]

The mandatory biometric SIM registration and the compulsory linking with the National Identity Number compromises anonymity online. Likewise, the excessive mandatory retention of communication data under different laws weakens

[188] Funmi Odude, 11 February 2021: "Illegality of the directive on NIN-SIM card linkage", http://www.financialnigeria.com/illegality-of-the-directive-on-nin-sim-card-linkage-blog-607.html accessed on 27 august 2021

[189] Ayang Macdonald Feb 2, 2021: "Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit, https://www.biometricupdate.com/202102/nigerias-move-to-link-digital-identity-numbers-to-sim-cards-sparks-lawsuit accessed on 27 august 2021

[190] Ayang Macdonald May 13, 2021: Nigeria reiterates the crucial role of national biometric ID, updates SIM registration policy https://www.biometricupdate.com/202105/nigeria-reiterates-crucial-role-of-biometric-national-id-updates-sim-registration-policy

[191] Nigerian Military Targeted Journalists' Phones, Computers with "Forensic Search" for Sources (*Committee to Protect Journalists*, 22 October 2019) <https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/> accessed 22 October 2021.

anonymity. According to the Declaration of Principles on Freedom of Expression and Access to Information in Africa,

> *Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies.*
>
> *The adoption of laws prohibiting encryption or of other measures that weaken encryption, including backdoors, key escrows, and data localisation requirements, are permissible only where justifiable and compatible with international human rights law.*

Mandatory SIM registration and the combination with NIN have been shown to negatively impact anonymity which is necessary to enjoy the right to protect one's personal information and freedom of expression.[192] The introduction of the policies highlighted above could threaten freedom of expression and protection of personal information by impeding journalists from carrying out their work which largely involves holding state and non-state actors accountable for violations.[193] This often plays out in that 'restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas and undermines the ability to communicate anonymously, organise and associate with others.

[192] 'Unlawful SIM Card Validation Exercise is a Threat to Anonymity And Privacy' (*Unwanted Witness*, 12 December 2017) <https://www.unwantedwitness.org/unlawful-sim-card-validation-exercise-is-a-threat-to-anonymity-and-privacy/> accessed 22 October 2021.

[193] 'Two Sides of the Same Coin – the Right to Privacy and Freedom of Expression' (*Privacy International*) <http://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression> accessed 22 October 2021.

5.0

Forward-Looking Practices: Safeguards and measures to address regulatory gaps.

5.1 Regulatory Gaps

The Nigerian data protection landscape is experiencing rapid development that was catalysed by the launching of the National Digital Economic Policy (NDEPS 2020 – 2030) by President Muhammed Buhari.[194] The initiative has produced many laudable laws and policies, but the regulatory landscape remains plagued by certain ills despite these advancements. A prevalent challenge appears to be the lack of political will on policymakers and the Nigerian government, as demonstrated by the fragmentation of the landscape and minimal implementation of data protection provisions in the different relevant laws.[195] In addition, efforts at harmonisation are slow, uncoordinated and ineffectual. Another challenge is that it is apparent that policymakers have a superficial understanding of the concept of data protection and thus lack the expertise required to design laws that are fit for domestic needs and purposes.[196] For example, the NDPR, which remains the superintending law on data protection in the country, is a copy and paste albeit shorter version of the European GDPR, with very little distinction as to suggest the recognition of domestic needs and peculiarities before its adoption.

The low level of awareness on the part of the general public remains a major challenge. Makulilo noted that Africans generally suffer from "privacy myopia", which means that they underestimate the value of their personal data and the need to secure its protection. In other cases, some are aware but cannot just be bothered.[197] Other challenges include the ignorance or disregard by data controllers to their obligations in the NDPR, lack of internal privacy awareness, frameworks or protocol, lack of clarity on data loss and breach, among other

[194] Inyene Ibanga (18 May 2021): Powering Nigeria's Digital Literacy Journey, By Inyene Ibanga, https://www.premiumtimesng.com/opinion/462240-powering-nigerias-digital-literacy-journey-by-inyene-ibanga.html, accessed on 29 August 2021

[195] Abdulrauf, L.A., Fombad, C.M. Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms. Liverpool Law Rev 38, 105–134 (2017). https://doi.org/10.1007/s10991-016-9189-8, pg 17

[196] Gwagwa notes this in relation to Africa generally. A. Gwaga et al. "Protecting the right to privacy in Africa in the digital age", http://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in- Africa-in-the-digital-age.pdf, accessed 27 August 2021.

[197] Alex B. Makulilo: "A Person Is a Person through Other Persons"—A Critical Analysis of Privacy and Culture in Africa, Beijing Law Review, Vol.7 No.3, August 22, 2016

things.[198] Also, the suitability and independence of the industry regulator, NITDA, is questionable, considering that it is a government parastatal wholly subject to the control of the Federal Ministry of Information and Digital Economy. Also worth mentioning is that the NDPR itself is subsidiary legislation that carries less weight than a data protection law.[199]

A significant regulatory gap concerning the legality or otherwise of NITDA to impose and collect administrate fines was also highlighted in the light of the Soko Loans regulatory action.[200] It has been argued that the NDPR and NITDA Act do not expressly confer this power on NITDA because by law, fines are criminal sanctions, and only a criminal court of competent jurisdiction can impose them after a trial and finding of guilt.[201] However, the 2020 Framework empowers the NITDA to impose a monetary fine, a sequel to a finding of breach of the NDPR in an administrative process guided by the nature, gravity and severity of the breach and number of affected data subjects.[202] Note that the Interpretation Act also confers authority to impose monetary punishments on a body empowered to make subsidiary legislation, provided that the punishment does not exceed an imprisonment term of 6 months or a one hundred Naira fine.[203] Read conjunctively, the powers of NITDA to impose a fine may be nonexistent or severely limited and subject to conflicting judicial and statutory precedents.

5.2 Safeguards and Measures to Address Regulatory Gaps

The most decisive step towards strengthening the Nigerian data protection landscape and plugging the current regulatory gaps in the framework would be the passage of the draft Nigerian Data Protection Bill 2020 into law. The Bill is a multi-stakeholder proposition for the country to have a national law on data protection and related matters. It builds on the NDPR by conforming to international standards, notably the European Union's GDPR, and creates a more comprehensive framework for protecting personal information safeguards, a factor instrumental to the

[198] Yemi Adeniran (20 Jan 2021) Data protection in Nigeria – enforcement in post-COVID-19 digital economy https://www.biometricupdate.com/202101/data-protection-in-nigeria-enforcement-in-post-covid-19-digital-economy accessed on 27 July 2021

[199] Bisola Scott & Sandra Eke, Nigeria: A Review of the Nigerian Data Protection Bill 2020, MONDAQ (Sept. 8, 2020), https://perma.cc/LWN9-UR4G.

[200] Aluko & Oyebode (August 2021): "Legality of the Imposition of a Fine on Soko Lending Company by the National Information Technology Development Agency", https://www.aluko-oyebode.com/wp-content/uploads/2021/09/Legality-of-the-Imposition-of-a-Fine-on-Soko-Lending-Company-Limited-by-the-National-Information-Technology-Development-Agency_.pdf, accessed on 28 August 2021

[201] See Abdullahi v. Kano State (2015) LPELR 25928

[202] See Article 10.1.4 of the NDPR Implementation Framework 2019

[203] Section 12(1)(c)(ii) of the Interpretation Act, Cap I23, LFN 2004

government's objective of boosting international trade and the IT sector.[204] The Federal Government introduced it through the Legal and Regulatory Reform Working Group (LWG) constituted in March 2020 as part of the government's efforts to implement the Nigeria Digital Identification for Development (ID4D) Project.[205]

One of the revolutionary features of the draft law is the proposed establishment of a distinct and recognised supervisory authority to be known as the Data Protection Commission. This is to be administered by a Governing Body. The Commission is tasked with implementing and monitoring compliance with the provisions of the Bill, making administrative arrangements necessary to the performance of its tasks, investigating complaints arising from the Bill, making regulations, applying for court warrants, imposing fines and penalties, and generally performing its duties with the support of law enforcement agencies.[206] The Data Protection Bill, if passed into law, would consolidate the existing framework and provide the basis of a strong data protection regime in the country.

Another measure that would prove effective in addressing regulatory gaps in the framework would be increased activity in the enforcement regime of the NDPR and other relevant laws that prescribe sanctions for violation of privacy obligations. However, there may be a need to fix the inherent flaws in the NDPR that constitute a clog to the success of the Regulation. While The NDPR 2019-2020 performance report reveals that NITDA has stepped up in its implementation, monitoring and enforcement drive, especially highlighted by the number of compliance and enforcement notices issued during the year in review and the fines recently imposed on three organisations.

The regulatory fragmentation in the Nigerian data protection landscape also emphasises the need for cooperation, harmonisation and partnerships in policymaking and relevant industry stakeholders, including the government agencies tasked with administering applicable laws that impact data protection across thematic areas. On a positive note, the NITDA is focusing on fostering these partnerships by facilitating in several meetings aimed at fostering better cooperation and harmonisation in the banking sector, the results of which appear to be paying off as the banking sector accounted for 36.3% of all filings recorded in the 2019 – 2020 compliance year. Other partnership projects include data protection cooperation with the Security and Exchange Commission (SEC) and

[204] Jeremy Daniel (26 October 2020) Nigeria Data Protection Bill aims to reinforce information security rules, https://www.cio.com/article/3586844/what-you-need-to-know-about-nigerias-new-data-protection-bill.html, accessed on 29 Jan 2021

[205] Bisola Scott and Sandra Eke (supra)

[206] ibid

Government MDAs. In addition, in November, NITDA and the Federal Competition and Consumer Protection Commission (FCCPC) announced collaboration on enforcement activities to regulate the activities of digital lending companies in the face of prevalent pervasive practices.[207] Also worthy of note is the NITDA's membership of the Policy and Regulatory Initiative for Digital Africa (PRIDA) working group on Data Protection Laws Harmonisation and Localisation facilitated by the AU Commission. NITDA serves as the Vice-Chair of the Group, comprising representatives of 16 African countries and the EU Commission.[208]

[207] Money Lending: CBN, EFCC, FCCPC, Others to Tackle 'Loan Sharks' (*Premium Times Nigeria*November 15, 2021) <https://www.premiumtimesng.com/news/top-news/495497-money-lending-cbn-efcc-fccpc-others-to-tackle-loan-sharks.html> accessed November 26, 2021.

[208] Emmanuel Elebeke (12 August 2020) "Africa: Nigeria Leads Africa in Data Protection, Despite Low Awareness - NITDA DG", https://www.vanguardngr.com/2020/08/nigeria-leads-africa-in-data-protection-despite-low-awareness-nitda-dg/ accessed on 29 August 2021

6.0
Recommendations

The following are the recommendations from this report for state actors, policymakers and legislators, and non-state actors like civil society organisations and activists, researchers, academia, and philanthropic organisations.

For Policymakers and Legislators

- There is a need for data protection to be recognised as a human right and cloaked with the priority protection availed to fundamental rights. The ideal starting point would resolve the confusion surrounding the dichotomy between privacy and data protection in the Nigerian context. There are two schools of thought on this issue: the first school posit that data protection conceptually differs from privacy and should be treated as such. The second argues that data protection derives from the constitutional right of privacy, despite its commercial influence, and should therefore enjoy protection under the relevant section of the Nigerian Constitution. Although the Nigerian appellate court has stated that data protection falls under the purview of Section 37, a legislative amendment recognising data protection as a fundamental right would conclusively lay the argument to rest.
- Policymakers and legislators should take a decisive step towards strengthening the Nigerian data protection landscape and plugging the current regulatory gaps in the framework by passing Data Protection legislation. They should also ensure the combined efforts of all stakeholders towards a timely production of comprehensive legislation.
- Provisions on 'journalistic exceptions' should be included in applicable laws and the draft Data Protection Bill, 2020 or any subsequent version of the proposed data protection law.
- There is a need to establish an independent Data Protection Commission. Currently, NITDA is a government agency under the purview of the Ministry of Information and Digital Economy, a parastatal of the executive arm of the government. This is contrary to international best practices, as Data Protection Authorities are expected to be independent and free from executive control to optimally and impartially discharge their duties. Unfortunately, this anomaly is present in the draft Data Protection Bill as the appointment, supervision, discipline, remuneration and removal of the members of the prospective regulator, the Data Protection Commission (DPC), would be at the pleasure of the President.

- The Lawful Interception of Communications Regulations should be amended to ensure law enforcement agencies cannot access encrypted communications without judicial review. In addition, the provisions of Section 45(2)(f) of the Cybercrimes Act of 2015 should be reviewed to provide a judicial review of the powers of law enforcement agencies to decrypt encrypted information. Also, the provisions in the Lawful Interception of Communications Regulations and Cybercrimes Act restricting anonymity should be repealed.
- The various laws on surveillance should be reduced into a single law. In addition, the provision should provide additional safeguards like allowing the notification of individuals who are subject to surveillance to contest it, institutionalising an independent oversight institution to monitor activities of investigating authorities, the mandatory requirement to conduct human rights impact assessment and data protection impact assessment before deploying surveillance tools, and the obligation on law enforcement agencies to notify the data protection authority when they suffer a data breach.
- Forward-looking legislation like the Digital Rights and Freedom Bill should be passed into law.

For Government

- There should be cooperation, harmonisation and partnerships in policymaking between relevant industry stakeholders, including the government agencies tasked with administering applicable laws that impact data protection across thematic areas.
- There is a need to strengthen the Nigerian courts through more training and independence to uphold existing laws.
- There is a need for the rule of law to be guided by internationally set human rights standards and the Nigerian Constitution.
- The Nigerian government must acknowledge and honour its commitments under regional and sub-regional instruments on data protection or complete the requirements necessary to apply these at a domestic level, especially with the coming into force of the African Continental Free Trade Agreement (AfCFTA). For instance, Nigeria is yet to ratify the AU Convention on Cyber Security and Data Protection and does not fully respect its obligations under the ECOWAS Supplementary Act on Data Protection which is already legally binding on it as a party to the ECOWAS Treaty. Operationalising these regional and sub-regional instruments would foster international synergy on data protection and data flows, strengthen the domestic framework and optimise the effectiveness of the regulatory framework.

- There should be an increased effort in the enforcement regime of the NDPR and other relevant laws that prescribe sanctions for violation of data protection obligations.
- Avenue for awareness and training to policymakers for a much broader rather than a superficial understanding of the concept of data protection and the expertise required to design laws that fit domestic needs and purposes.
- The regulatory fragmentation in the Nigerian data protection landscape and the minimal implementation of data protection provisions emphasises the need for the government and policymakers to portray the requisite political will.
- Institutions should be adequately funded to fulfil their statutory mandate.
- The Attorney-General of the Federation and law enforcement agencies should publish a transparency report publicly on the extent of surveillance conducted and the number of requests made to service providers.

For Civil Society Organisations and Activists

- There must be efforts to increase awareness among stakeholders. For instance, in a survey conducted in July 2020, respondents rated the public awareness rate of data protection at 54%. Therefore, it could be presumed that more Nigerians would be more alert and inclined to enforce data protection rights if they were better enlightened about the potential risks in the unregulated processing of their personal information. Therefore, a multi-stakeholder approach, comprising public and private bodies, is needed to raise awareness among the general public with sufficient training, scholarship, policymaking.
- Civil Society Organisations and Activists should monitor the governments' compliance with the rule of law.
- There is a need to demand greater accountability and transparency from the government through constant engagement, using access to information laws.
- Creation of awareness to the general public about the value of their personal data and the need to secure its protection.
- There should be increased strategic litigations to challenge government excesses and the provisions of certain laws that restrict or derogate from international human rights principles.

For Researchers, Academia and Philanthropy Organisations

- They should act as bridges between quality research and policy reform.
- It is recommended that they carry out more contextually relevant research on the need for comprehensive legislation.

- Research should be conducted to highlight the gaps in the regulation and the operationalisation of the law. Research should also be conducted to understand the extent of violation of the right and the impact on people.
- Research is needed to fully understand the extent of government surveillance often clogged in opaqueness.

7.0
Conclusion

In this report, a holistic appraisal has been attempted of the operative Nigerian data protection landscape, including the current structure of the framework as well as its impact across the legal and regulatory legal framework of thematic areas such as digital and biometric identity, surveillance, freedom of expression, data breach and violations, encryption and anonymity, cybercrime and cybersecurity. The regulator's multifaceted roles in the framework, the challenges militating against enforcement and regulatory reforms, and the efforts and accomplishments of the data protection regulator are emphasised. Recommendations are on the proper future direction of the landscape are also proffered. The Nigeria Data Protection Regulation Performance Report 2O19-2O2O reveals that despite the developing status of data protection, a blueprint is being established for increased efficiency in the coming years.

While significant strides have been recorded in the rapidly evolving data protection ecosystem, it is clear that the current framework is no match for private and public activities in surveillance, curtailment of freedom of expression, digital identity schemes, vague and excessive data processing and retention, data localisation, government registration, data breaches, cybersecurity and related issues. Therefore, it is necessary that the current legal framework, policies and practices guiding these issues be reviewed and reformed to bring them in conformity with international human rights standards and demonstrate the application of the principles of necessity, legality and proportionality. The type, financial costs, and use of the government's surveillance tools should be disclosed and regulated. Thorough and independent investigations should be conducted into reports of violations and publicised to stop perpetrators and make reparations to victims.[209]

Efforts in this regard should be geared and supported by the government and relevant stakeholders, including corporate bodies, civil societies, and relevant individuals. Adopting and implementing these tough but progressive steps would be a loud and affirmative statement of Nigeria's intention to advance its data protection approach to international standards and efficiently compete in the digital economy.

[209] Paradigm Initiative (March 2018): The Right to Privacy in the Federal Republic of Nigeria, Stakeholder Report Universal Periodic Review 31st Session – Nigeria, pg 12

OMIDYAR NETWORK
TECH HIVE ADVISORY
PARADIGM INITIATIVE