accountabilitylab NIGERIA

A COMPENDIUM ON DIGITAL GOVERNANCE AND THE CITIZEN: POLICY, PROTECTION, AND PRACTICE IN NIGERIA

ACKNOWLEDGEMENT

We extend our sincere gratitude to all contributors whose expertise and dedicated efforts were instrumental in the development of Digital Governance and the Citizen: Policy, Protection, and Practice in Nigeria. Their rigorous research and valuable insights fundamentally shaped the substance of this work.

Our special thanks are due to Professor Jake Okechukwu Effoduh, Assistant Professor at the Lincoln Alexander School of Law, Toronto Metropolitan University, Canada, whose exemplary leadership of the editorial and review process, meticulous scrutiny, and constructive feedback significantly enhanced the quality of this publication.

We further acknowledge the invaluable support of institutions, practitioners, and digital rights advocates whose work informed the analyses and perspectives presented in this compendium.

Finally, we express our appreciation to everyone who contributed through support, review, and encouragement throughout the publication process. Your collective contributions made this work possible.

Table of Contents

PART ONE

IDENTITY AND FOUNDATIONAL DIGITAL RIGHTS

CHAPTER 1

Digital Identity Behind Custodial Walls: Evaluating the Benefit of Mandatory National Identity Number (NIN) Enrollment of Inmates in Nigeria

by

IGOMU, Joseph Augustine PhD
Nigerian Correctional Service Abuja, Nigeria
AUS American Institute of Applied Sciences, Switzerland

Email: igomufreeman8@gmail.com

Abstract

Nigeria's expansion of the National Identity Number (NIN) into custodial centres/facilities links a vulnerable population to the country's core digital infrastructure. The Nigeria National Identity Management Commission (NIMC) has commenced the implementation of mandatory National Identity Number (NIN) enrollment for inmates within the custodial centres/facilities of the Nigerian Correctional Service (NCoS), raising new questions about rights, reintegration, and security. This paper evaluates the benefits and limitations of mandatory NIN enrollment for inmates, with a focus on post-release reintegration, surveillance, recapture, and human rights. It draws on administrative data, legal instruments, and secondary sources to examine how digital identity systems interact with criminal justice, data privacy, and civic inclusion. Findings show that while the NIN initiative enhances documentation and access to public records, it risks surveillance creep, exclusion, and loss of personal agency without strong oversight and inclusion-first design. The paper concludes with a multi-stakeholder, rights-respecting framework for inmate digital identity governance in Nigeria, providing actionable insights for policymakers, correctional administrators, and digital-rights advocates.

Context and Rationale

Nigeria's digital governance landscape has undergone a significant transformation in recent years, with the National Identity Management Commission (NIMC) spearheading a large-scale biometric identity programme. Established by the NIMC Act No. 23 of 2007, NIMC has the mandate to establish, own, operate, maintain and manage the National Identity Database in Nigeria, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to citizens and lawful residents where applicable. The NIN has evolved into core infrastructure for accessing government services, financial inclusion, and civic participation. NIMC's enrolment figures as at June 30, 2025 currently stand at over 121,404601 in millions (enrolment distribution by gender, male: 68,481,392 females: 52, 923, 209) Nigerians and legal residents have been enrolled in the Commission's database (NIMC, 2025).

Nigerian Data Protection Regulation (NDPR) 2019, part two 2.1. The regulation makes provision for the governing principles of data processing and it provides that in addition to the procedures laid down in the regulation or any other instrument for the time being in force, personal data shall be: (1) In addition to the procedures laid down in this regulation or any other instrument for the time being in force, personal data shall be: a) collected and processed in accordance with specific, legitimate and lawful purpose consented to by the data subject; provided that: i. a further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest; ii. any person or entity carrying out or purporting to carry out data processing under the provision of this paragraph shall not transfer any personal data to any person; b) adequate, accurate and without prejudice to the dignity of human person; c) stored only for the period within which it is reasonably needed, and d) secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements (NDPR, 2019).

The NIN registration exercise is mandatory for all inmates, regardless of prior enrolment status. The National Identity Management Commission system is capable of detecting previous enrolments, ensuring that duplicate registrations do not occur (NCoS Radio Message, 2025). It is imperative to emphasize that the capture of biometric and other inmate data is a core mandate of the Nigeria Correctional Service, as stipulated in Section 13 (1) (d) of the NCoS Act 2019. Furthermore, Section 13 (4) (b) of the Act Mandates Officers-in-Charge to ensure proper documentation of inmates under their supervision (NCoS Act, 2019).

The extension of mandatory NIN enrollment to inmates in the custodial centres of the Nigerian Correctional Service (NCoS) marks a significant intersection of digital identity and criminal-justice policy. This initiative, implemented as part of Nigeria's broader digital identity strategy, reflects the federal government's commitment to comprehensive identity coverage while raising fundamental questions about lawful basis, oversight, and the balance between administrative efficiency, security imperatives, and the protection of fundamental rights for vulnerable populations. The Nigerian Correctional Service, transformed through the Nigerian Correctional Service Act of 2019, manages 81,349 inmates (male 79,470 and female 1,879) across two hundred and fifty-six (256) custodial centres/facilities in Nigeria as at September 2025 (NCoS, 2025).

NIMC has successfully enrolled 59,786 inmates across custodial centres/facilities in Nigeria (NIMC, 2025). The NCoS Act signals a paradigm shift from punitive imprisonment to rehabilitation and reintegration, emphasizing the importance of preparing inmates for successful reintegration into society. Section 14 (1) of the Act mandates that "the Correctional Service shall provide opportunities for education, vocational training, as well as training in modern farming techniques and animal husbandry for inmates" (NCoS Act, 2019).

The mandatory NIN enrollment initiative offers operational gains (record integrity, identity verification, recapture support), which emerge as both an opportunity to enhance administrative efficiency and a mechanism for tracing of inmates after escape and can support post-release reintegration when embedded in discharge planning. (NCoS, 2025). However, the implementation of digital identity systems in a custodial environment presents distinct challenges, such as limited agency, heightened privacy concerns, and complex legal statuses, that complicate standard identity workflows. The custodial environment also heightens risks around data protection and surveillance creep.

Internationally, experiences are mixed; while some jurisdictions have reported improved inmate management and reintegration outcomes, others document data-security failures, privacy violations, and exacerbated inequalities. The policy lesson is to pair enrollment with explicit safeguards, inclusion measures, and independent oversight. Nigeria's circumstances include an evolving data-protection framework, resource-constrained facilities, and broader socio-economic barriers to re-entry. Understanding these dynamics is necessary to ensure the policy achieves its goals and avoids foreseeable harms.

Problem and Evidence Gap

Despite nationwide rollout in custodial centres/facilities, the policy lacks a consolidated, public evaluation of its effects on rights, operations, and post-release outcomes.

As a result, guidance for implementation is fragmented, frameworks for protecting inmate digital rights are unclear, and mechanisms to ensure the system advances rehabilitation, reintegration, and service access remain underspecified. Reports indicate that the exercise is facing significant resistance in various custodial centres. Some of the inmates are refusing to participate, citing prior enrollment before incarceration as their reason (NCoS Radio Message, 2025).

The problem is compounded by four factors:

- Vulnerability and limited number of the inmate population;
- Legacy constraints within NCoS;
- Technical and procedural demands of biometric systems; and
- Gaps in the legal and regulatory framework.

The connection of multiple complex factors: the vulnerability of the inmate population, the historical challenges of Nigeria's correctional service, the technical requirements of digital identity systems, and the wider context of Nigeria's evolving digital governance. Current implementation lacks a comprehensive assessment of impacts on inmate experience, discharge planning, and correctional-reform objectives.

The major knowledge gaps include:

- Effectiveness against stated objectives;
- User experience (inmates and staff) and failure/error modes;
- Adequacy of legal bases, safeguards, and redress; and
- Distributional impacts on inclusion and equity.

Furthermore, interactions with known barriers to re-entry (documentation, banking, SIM, IDs) remain under-exploited without systematic evaluation and enforceable safeguards. Foreseeable risks include surveillance creep, exclusion, and new forms of discrimination.

Objectives of the Paper

The overall objective is to assess the implementation, benefits, and challenges of mandatory National Identity Number enrollment for inmates in custodial centres/facilities of the Nigerian Correctional Service, with a view to informing human rights, digital inclusion, and post-release reintegration. This paper specifically seeks;

- To analyze the institutional processes and policy rationale underlying the implementation of mandatory NIN enrollment for inmates in Nigerian custodial centres/facilities;

- To assess operational benefits and failure modes (e.g., enrollment errors, refusals, data-quality issues) and their impact on reintegration;

- To examine the intersection of digital surveillance and inmate rights in Nigeria, the evolving legal framework for data protection and digital governance;

- To propose recommendations for developing inclusive, rights-respecting digital identity governance frameworks for inmates in Nigeria.

Literature Review

Digital Identity and Governance in Nigeria

The World Bank's Identification for Development 2016 popularly known as the (ID4D) initiative; brings global knowledge and multi-sectorial expertise to help countries realize the transformational potential of digital identification (ID) systems. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal issues. One obtainable digital identification project in West Africa is the West Africa Unique Identification for Regional Integration and Inclusion (WURI) programme initiated by the World Bank under its ID4D initiative. The WURI programme is to serve as an umbrella under which West African States that collaborate with the Economic Community of West African States (ECOWAS) to design and build a digital identification system, financed by the World Bank, that would create foundational IDs (fID) for all persons in the ECOWAS region. Many West African States that have had past failed attempts at digitizing their identification systems have embraced assistance via WURI.

Digital identity is a set of validated digital attributes and credentials applicable in the digital world, like a person's identity for the real world. digital identity serves to uniquely identify a person on-line or off-line. Having defined digital identity, digital identification, simply put, has at its core the verification, confirmation, ascertainment of an alleged identity online. Digital identification often indicates a process; it is a better term to describe a proof, a system, or a transaction involving a subject and an evaluator, centered around verifying a claim that a person is one person and not any other. It also works well when referring to the recording of certain attributes like biodata, biometrics, claims in a formal record, a "credential," that grants specific rights or permissions to the individual (Digital Rights Lawyers, 2021). Digital identity constitutes a verifiable, electronic representation of an individual's personal attributes, credentials, and characteristics that can be electronically verified and authenticated within digital systems (Whitley, 2018).

From a custodial perspective, digital identity encompasses biometric data, personal identifiers, and authentication mechanisms that facilitate the secure identification and record-keeping of incarcerated individuals. Contemporary correctional services rely on digital identity systems for inmate management, utilizing biometric fingerprint (e.g., fingerprint) identification technology and digital credentials to register and identify millions of inmates annually.

The conceptualization of digital identity in custodial environments extends beyond post-release outcomes and civic participation. Digital identity is often a prerequisite for accessing government services such as, basic IDs, SIM reactivation, employment opportunities, and social benefits upon release from incarceration (U.S. Government Accountability Office, 2023).

The literature on digital identity systems in low- and middle-income countries reveals both opportunities and risks. Elb and Diofasi (2020), argue that digital identity systems can be transformative for development outcomes, improving service access, reducing fraud, and increasing administrative efficiency, conditional on inclusive design principles, clear lawful bases, strong legal frameworks, and adequate technical infrastructure. On digital identity systems in Africa, highlight both the potential for these systems to advance development goals and the risks they pose to human rights and social inclusion.

Their analysis reveals that while digital identity enhances service delivery and economic participation, it can also exacerbate existing inequalities and create new forms of exclusion, particularly for vulnerable populations.

Studies of Nigeria's digital identity ecosystem specifically have noted both progress and persistent challenges. NIN system has achieved significant enrollment numbers, implementation has been uneven, with particular challenges in rural areas and among vulnerable populations.

The importance of addressing infrastructure gaps, digital literacy, and privacy concerns to ensure inclusive implementation.

Custodial-specific literature remains limited, but adjacent studies on digital identity in constrained settings underscore recurrent issues, which include lawful basis for processing sensitive biometrics, purpose limitation, retention schedules, access controls, and effective redress mechanisms. These dimensions are directly relevant to NCoS/NIMC workflows and inform the policy analysis in this paper.

Custodial Walls and Digital Technology

The term “custodial walls” represents both the physical and metaphorical barriers that characterize correctional institutions and their operational frameworks. From a physical perspective, custodial walls signify the structural restrictions that define correctional facilities, creating controlled environments where imprisoned individuals are housed under state supervision. Metaphorically, these walls represent systemic barriers that impede the integration of imprisoned populations into larger societal and administrative systems. The integration of digital technology in the correctional service in Nigeria has received increasing attention.

National Identity Number (NIN)

The National Identity Number represents a unique numerical identifier assigned to Nigerian citizens and legal residents by the National Identity Management Commission as part of Nigeria's national identification system. According to NIMC regulations, the NIN serves as the primary identifier for accessing government services and is mandatory for all Nigerian citizens and legal residents (NIMC, 2024). Recent policy developments have extended NIN enrollment to custodial centres/facilities in Nigeria. The National Identity Management System (NIMS) is the infrastructure responsible for the management of the NIMC mandate. The benefits of NIMS are

- Uniquely identifying individuals;
- It provides a platform where no one is excluded socially or financially;
- It transforms the delivery of social welfare programmes, especially for those cut off from such benefits;
- It enables people to claim their entitlement;
- It helps eliminate duplicate identities and fraud;
- It reduces the cost of resources as infrastructures are shared.

Biometric Identification

Biometrics is defined as the collection of approaches and algorithms that are used for uniquely recognizing humans based on physical or behavioural cues (Ryan, Brett, Martin, & Shasha, 2023). Biometric identification involves the use of unique biological characteristics, such as fingerprints, facial features or iris patterns, for individual identification and authentication purposes. Within correctional environments, biometric identification systems serve as primary mechanisms for inmate identification, facility access control, and security management.

Mandatory Enrollment

Mandatory enrollment refers to the compulsory participation of specific population groups in Nigeria's identification systems as required by law. From the perspective of correctional facilities, mandatory enrollment represents a policy mechanism whereby imprisoned individuals are required to participate in national identification systems, regardless of their prior enrollment status or personal preferences. The implementation of mandatory NIN enrollment for inmates in Nigeria reflects broader governmental efforts to achieve comprehensive population coverage in national identification systems. The Nigerian Correctional Service has successfully enrolled over 73 per cent of inmates nationwide into the National Identity Management Commission database, demonstrating the practical implementation of mandatory enrollment policies within custodial settings.

Human Rights and Digital Identity

The human rights implications of digital identity systems have become a focal point of academic and policy attention in the twenty-first century. Privacy International (2021) argues that digital identity systems can violate fundamental rights to privacy, freedom of movement, and non-discrimination if not properly designed and implemented.

Their analysis emphasizes the particular vulnerabilities of marginalized populations, including inmates, who may have limited ability to resist or challenge digital identity requirements. Digital identity systems implemented in correctional environments must include strong safeguards against mission creep and ensure that data collected for administrative purposes is not used for other intentions.

Legal Framework for Biometric Data Processing in Custodial Settings in Nigeria

The processing of inmate biometric data in Nigerian correctional facilities operates within a transformed legal framework established by the Nigeria Data Protection Act 2023 (NDPA). Section 30 (2) of the NDPA explicitly classifies biometric data as sensitive personal data requiring heightened protection, while Section 29 establishes the foundational principles governing data controllers' and processors' obligations when determining the purpose and manner of data processing. The NDPA provides specific derogations applicable to custodial environment. Section [X] permits processing by competent authorities for crime prevention, investigation, prosecution, or enforcement of penalties under applicable laws, establishing the lawful basis for mandatory NIN enrollment. However, this statutory derogation does not obviate data protection principles; rather, it modifies their application within criminal justice system frameworks.

Lawful Bases for Inmate Processing

- The Nigerian Correctional Service Act 2019, Section 13(1) (d) and 13(4) (b), explicitly mandates biometric data capture and proper documentation of inmates, creating a statutory foundation that interfaces with NDPA competent authority derogation;

- Processing must be demonstrably necessary for the specific statutory purpose and proportionate to the objective sought, precluding function creep or secondary uses without separate legal authorization;
- Post-release reintegration and administrative efficiency constitute legitimate public interest objectives, provided they are explicitly articulated, legally authorized, and subject to procedural safeguards.

Data Subject Rights and Limitations

The NDPA recognizes that certain data subject rights may be restricted in custodial environment:

- Inmates retain the right to request information about data processing, though operational security may justify limited disclosure of system architecture or security measures;
- Inmates must have mechanisms to correct inaccurate biometric or biographical data, as errors directly impact post-release service access;
- Unlike general data subjects, inmate data retention extends beyond consent withdrawal due to statutory mandates for criminal records and recidivism tracking. However, retention schedules must be specified, and deletion protocols established for non-statutory data;
- The mandatory nature of NIN enrollment effectively suspends the general right to object, yet this derogation requires explicit statutory authorization and must be interpreted narrowly to prevent abuse.

Regulatory Oversight and Enforcement

The Nigeria Data Protection Commission serves as the primary oversight authority, with powers to:

- Investigate complaints regarding unlawful processing in custodial settings;
- Issue compliance directives to NCoS and NIMC;
- Impose administrative sanctions for violations of data protection principles;
- Conduct audits of biometric enrollment systems in correctional facilities.

Redress Mechanisms

The NDPA establishes multi-tiered redress mechanisms:

- NCoS must designate Data Protection Officers responsible for receiving and investigating inmate complaints regarding enrollment processes, data accuracy, or alleged misuse.
- Inmates or their legal representatives may lodge formal complaints with the Commission, triggering independent investigation and potential enforcement action.
- Constitutional challenges to mandatory enrollment or alleged violations of fundamental rights remain justiciable before Nigerian courts, providing ultimate recourse for systemic grievances.

The Relationship Between NDPA 2023 and NDPR 2019

The NDPR 2019 functions as a subsidiary regulatory instrument operating under the NDPA statutory framework. Where NDPR provisions conflict with the Act, the NDPA statutory provisions supersede the regulation. However, NDPR guidelines on data security, breach notification, and impact assessments retain interpretive value for operationalizing NDPA requirements in correctional contexts.

Gaps Requiring Legislative Clarification

The NDPA and its implementing regulations do not offer specific guidance on how biometric data should be handled in coercive environments such as correctional facilities, leaving room for interpretive uncertainty. The law also fails to establish clear limits on how long inmate biometric data can be retained after release, creating the possibility of indefinite storage that runs counter to data minimization principles. In addition, the Act provides limited clarity on the legal authority and procedural safeguards for sharing NIN-linked biometric data among security agencies, which raises concerns about unchecked data sharing and potential surveillance overreach. Finally, it does not adequately protect the rights of former inmates to restrict or separate their criminal justice information from civil identity systems once they have completed their sentences.

Reintegration and Social Inclusion

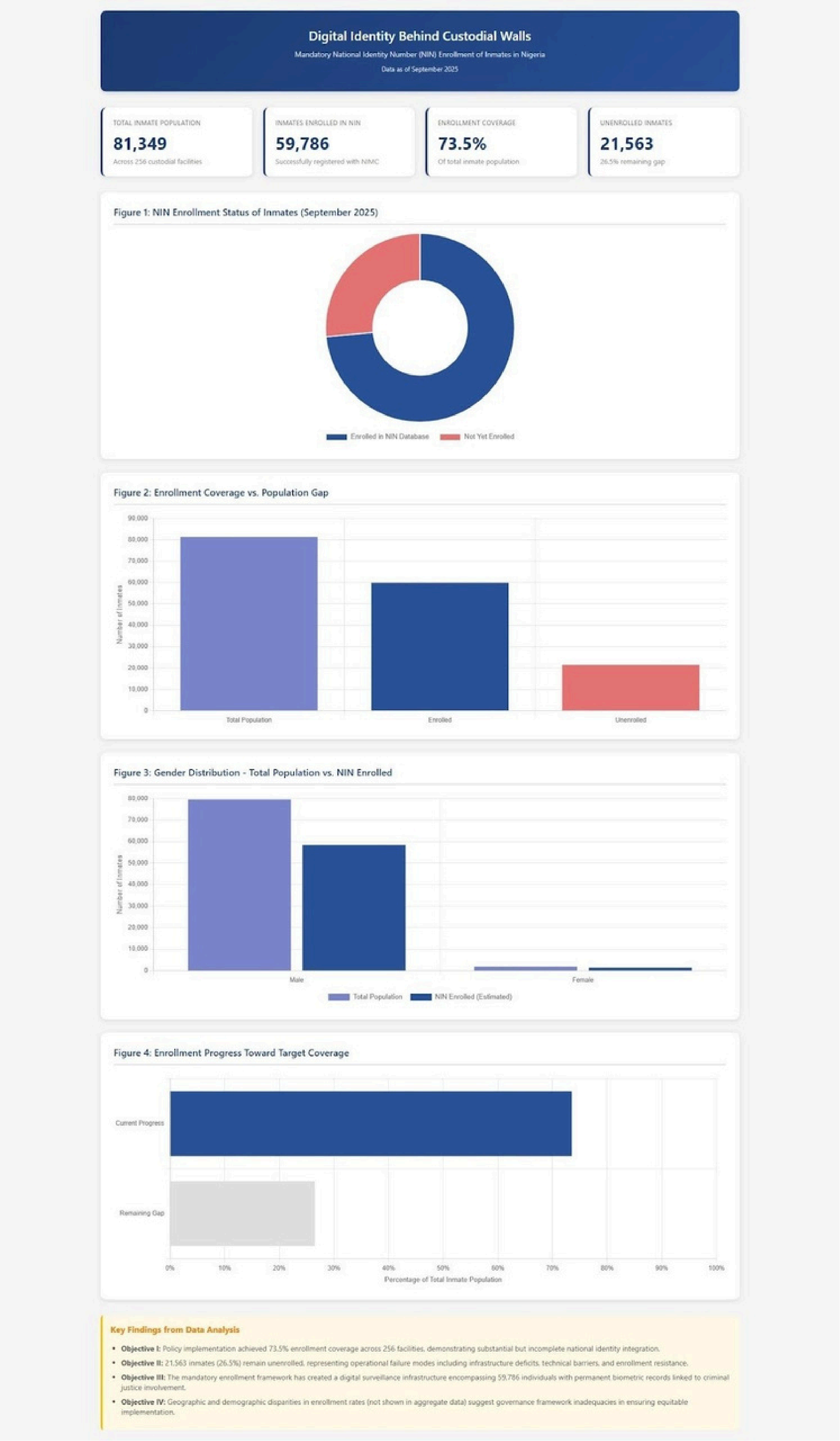
Reintegration includes the process through which formerly imprisoned individuals transition back into society, resuming participation in economic, social, and civic activities. Digital identity plays a vital role in facilitating successful reintegration by providing access to essential services and opportunities. The literature on inmates or prisoner reintegration in Nigeria identifies multiple barriers to successful reintegration, including stigmatization, lack of employment opportunities, and limited access to essential services. The importance of addressing these systemic barriers through comprehensive policy interventions that support former inmates' full participation in society.

Methodology and Data Sources

This study focusing on the Nigerian Correctional Service as the primary institution for evaluating the mandatory NIN enrollment of inmates. This study employs a qualitative document analysis and policy evaluation approach to assess the implementation, benefits, and challenges of mandatory NIN enrollment for inmates in Nigerian correctional facilities. The analysis synthesizes publicly available policy documents, administrative reports, media coverage, and academic literature to construct a comprehensive assessment of the policy implications for human rights, digital inclusion, and reintegration. The study employs a rights-based analytical framework assessing the policy.

The research draws on a wide range of publicly available materials, including government policies, administrative reports, academic studies, and media coverage. Key documents reviewed include the Nigeria Data Protection Act 2023, the Nigerian Correctional Service Act 2019, and the NIMC Act No. 23 of 2007, along with accompanying regulations, operational guidelines, and annual reports from the National Identity Management Commission (NIMC). Statements and press releases from the NCoS, as well as guidance from the Nigeria Data Protection Commission, were analyzed to track implementation progress and identify emerging issues.

To provide a balanced and rights-based perspective, the study also reviews secondary sources such as peer-reviewed articles on digital identity systems, reports on Nigeria's digital governance ecosystem, and human rights literature concerning data protection in custodial settings. These are complemented by case studies from international bodies such as the World Bank's ID4D initiative, Privacy International, and the U.S. Government Accountability Office on prisoner identification and reintegration. Together, these materials form the evidence base for evaluating how mandatory NIN enrollment in correctional facilities intersects with privacy, inclusion, and rehabilitation objectives in Nigeria.



Digital Identity Behind Custodial Walls

Mandatory National Identity Number (NIN) Enrollment of Inmates in Nigeria

Data as of September 2025

TOTAL INMATE POPULATION	INMATES ENROLLED IN NIN	ENROLLMENT COVERAGE	UNENROLLED INMATES
81,349	59,786	73.5%	21,563
Across 256 custodial facilities	Successfully registered with NIMC	Of total inmate population	26.5% remaining gap

Figure 1: NIN Enrollment Status of Inmates (September 2025)

Figure 2: Enrollment Coverage vs. Population Gap

Figure 3: Gender Distribution - Total Population vs. NIN Enrolled

Figure 4: Enrollment Progress Toward Target Coverage

Key Findings from Data Analysis

- **Objective I:** Policy implementation achieved 73.5% enrollment coverage across 256 facilities, demonstrating substantial but incomplete national identity integration.
- **Objective II:** 21,563 inmates (26.5%) remain unenrolled, representing operational failure modes including infrastructure deficits, technical barriers, and enrollment resistance.
- **Objective III:** The mandatory enrollment framework has created a digital surveillance infrastructure encompassing 59,786 individuals with permanent biometric records linked to criminal justice involvement.
- **Objective IV:** Geographic and demographic disparities in enrollment rates (not shown in aggregate data) suggest governance framework inadequacies in ensuring equitable implementation.

Source: Author Compilation (2025).

Discussion of Findings

Institutional Processes and Policy Rationale (Objective I)

Documentary evidence reveals that mandatory enrollment emerged from Federal Ministry of Interior directives as part of correctional service reform. Policy documents identify four motivations: administrative efficiency, inmate tracking, reintegration support, and comprehensive identity coverage (NIMC, 2024). However, development involved minimal staff consultation, reflecting top-down governance. Phased rollout prioritized urban correctional facilities, creating equity concerns as rural inmates experience delayed services. The mandatory requirement prioritizes database comprehensiveness over individual agency, raising proportionality questions in coercive environments.

Operational Benefits and Failure Modes (Objective II)

Administrative efficiency constitutes the most documented benefit. Reports indicate enhanced record-keeping, reduced identity fraud, and streamlined processes (NCoS, 2024). Duplicate detection addresses fragmentation in Nigeria's identification landscape. For reintegration, NIN possession facilitates banking, employment, and government service access, reducing bureaucratic barriers (U.S. GAO, 2023). The system enhances security through reliable identification supporting inmate tracking and recapture efforts. Multiple failure modes undermine benefits. Enrollment errors from poor biometric capture, inadequate training of personnel, or equipment malfunctions create problems with cascading consequences. Inmates with erroneous records face post-release verification hitches. Resistance patterns reveal inmates refusing enrollment despite prior registration claims (NCoS Radio Message, 2025). Insufficient information provision generates compliance challenges. Infrastructure deficits create physical inequities urban correctional facilities achieve more enrollment than rural correctional facilities. Vulnerable subpopulations (disabled, foreign nationals, illiterate) face heightened barriers. Overstretch correctional facilities creates exclusion risks, disregarding those most needing identification.

Legal Framework and Surveillance Implications (Objective III)

The NDPA 2023 transition strengthened protections by establishing statutory frameworks and creating the Nigeria Data Protection Commission. Section 30(2) classifies biometric data as sensitive, requiring heightened protection. NCoS Act 2019 Sections 13(1)(d) and 13(4)(b) create statutory mandates establishing lawful bases. However, gaps persist. Neither NDPA nor regulations provide custodial-specific guidance addressing coercive implications, consent limitations, or rights modifications. Retention schedules remain unspecified, enabling indefinite retention contrary to minimization principles. Cross-agency sharing procedures lack clear parameters, creating surveillance creep risks.

Integration into national infrastructure presents implications. It normalizes civic status and facilitates post-release participation. It also creates permanent records linking individuals to criminal justice. Inadequate purpose limitation and access controls heighten surveillance creep risks, where administrative data becomes repurposed for extended monitoring. Privacy International (2021) emphasizes that digital identity systems sometime can violate fundamental rights without adequate safeguards, particularly affecting marginalized populations. In custodial environments with structural power imbalances, these risks intensify.

Governance Framework Requirements (Objective IV)

Current governance inadequately balances administrative objectives with rights protection. Three serious deficits emerge:

- No independent mechanism monitors implementation. NDPC lacks custodial-specific procedures, resources, or expertise. NCoS monitoring focuses on coverage statistics rather than rights compliance or consequence assessment;
- Limited public reporting on processes, failure rates, complaints, or remedies constrains accountability. Absent impact assessments prevent evidence-based refinement and obscure unintended consequences;
- While NDPA establishes theoretical mechanisms, practical accessibility remains questionable. Some correctional facilities lack designated Data Protection Officers, inmates receive insignificant information, and reprisal fears deter complaints. These deficits undermine policy legitimacy and sustainability, risking devolution into compliance exercises prioritizing convenience over rehabilitation objectives.

Technical and Operational Challenges

The documentary evidence reveals infrastructural and operational constraints impeding effective NIN enrollment implementation in Nigerian Correctional Service. These challenges reveal wider systemic deficits affecting digital transformation in resource-constrained institutional environments.

Infrastructure Deficits

Persistent electricity shortages constitute a fundamental impediment to biometric enrollment operations. This deficit severely constrains custodial facilities' capacity to maintain continuous digital system operations. The Nigerian Correctional Service recent memorandum of understanding with the Rural Electrification Agency to deploy renewable energy infrastructure across custodial centres/ facilities highlights the severity of this constraint and its unfavorable impact on enrollment system functionality. Dependency on diesel generators imposes extra financial burdens while providing inadequate support for continuous biometric system operations, particularly during extended grid power failures.

Network Connectivity Limitations

Inadequate telecommunications infrastructure presents significant barriers to real-time biometric verification and database synchronization. Many custodial centres/facilities operate within these connectivity-challenged zones, creating operational inconsistencies across the correctional facilities. Urban facilities achieve higher enrollment rates and data quality compared to rural counterparts due to superior network infrastructure.

Technical Knowledge Deficits

Insufficient technical capacity among correctional personnel constitutes a human resource constraint. This capacity deficit manifests acutely in correctional facilities, where personnel traditionally trained in custodial and security functions must suddenly operate sophisticated biometric enrollment systems.

Maintenance System Inadequacy

This infrastructure deficit extends to maintenance capacity, with custodial centres lacking ICT support personnel, spare parts inventories, and service contracts with technology vendors. The centralization of technical support creates additional challenges for remote facilities. Equipment malfunctions necessitate external support requests, involving substantial delays due to distance, resource constraints. During system unavailability periods, enrollment activities cease, creating backlogs and undermining programme efficiency. The absence of preventive maintenance programmes further exacerbates equipment reliability challenges, as minor technical issues escalate into major system failures.

Recommendations

Based on the study findings, the following recommendations are proposed:

Legal and Regulatory Strengthening

- NDPC should promulgate subsidiary regulations addressing custodial and/or correctional facilities biometric processing, specifying: modified consent procedures acknowledging coercive contexts; enhanced information provision ensuring inmates understand implications; retention schedules mandating deletion within specified post-sentence periods absent separate authorization; and purpose limitation protocols prohibiting secondary uses without explicit legal bases;
- Establish multi-stakeholder committee (NDPC, NCoS, NIMC, civil society, legal experts, formerly incarcerated inmates) with statutory authority for unannounced inspections, complaint investigation, audit access, and binding recommendations. Annual public reporting should detail statistics, complaints, remedies, and compliance assessments;
- Amend NIMC Act or enact regulations defining circumstances, procedures, and limitations governing security agencies' access to inmates' NIN-linked data and other data. Establish judicial authorization requirements beyond administrative purposes, checking surveillance creep while preserving legitimate security applications.

Infrastructure and Capacity Development

- Allocate dedicated funding for: renewable energy ensuring continuous power; satellite/broadband connectivity enabling real-time synchronization; standardized ICT equipment with spare parts. Prioritize underserved rural correctional facilities addressing geographic equity deficits;
- Develop comprehensive training covering biometric capture in the correctional service.

Conclusion

The implementation of mandatory NIN enrollment for inmates in the Nigerian Correctional Service represents a significant development in the intersection of digital governance and criminal justice reform. While the policy has achieved some of its intended objectives, including improved administrative efficiency and enhanced access to identification documents for post-release reintegration, it has also revealed significant challenges related to digital rights, and suspending of some vulnerable populations where the equipment is weak. This study shows that the success of digital identity initiatives in correctional services depends heavily on the strength of legal frameworks, the adequacy of institutional capacity, and the extent to which human rights principles are integrated into policy design and implementation. The current implementation of the NIN enrollment policy in Nigeria reveals significant gaps in these areas, suggesting the need for comprehensive reforms to ensure that the policy serves its intended purposes while protecting the rights and dignity of inmates.

As digital technologies continue to evolve, so too must our understanding of their implications for human rights, social justice, and the achievement of development objectives. Only through sustained attention to these issues we ensure that digital governance serves the interests of all citizens, including those who are the most vulnerable.

References

Digital Rights Lawyers. Overview-of-digital-identity-and-digital-identification-in-nigeria-group-4-powerpoint.pdf 2021. https://digitalrightslawyers.org/wp-content/uploads/

Elb, A. & Diofasi, A., Digital identity systems and inclusive development: Opportunities and challenges for developing countries, Development Policy Review, vol. 38, no. 4, 2020, pp. 455– 472.

M2SYS Technology, 'Biometric Fingerprint Identification Technology Used to Register and Identify Millions of Inmates and Facility Visitors Each Year', 2024, https://www.m2sys.com/blog/biometric-identification-technology/biometric-fingerprint- identification-technology-used-to-register-and-identify-millions-of-inmates-and-facility- visitors-each-year/.

National Identity Management Commission (NIMC), Annual Report 2023: Progress in National Identity Management, Abuja: NIMC Publications, 2024.

National Identity Management Commission (NIMC), 'National Identity Management Commission Licenses Nigerian Correctional Service to Enroll Inmates for NIN', 2024, https://nimc.gov.ng/national-identity-management-commission-licenses-nigerian- correctional-service-to-enroll-inmates-for-nin/.

National Identity Management Commission Act No. 23 of 2007. Federal Republic of Nigeria. Government Press.

National Identity Management Commission. (2025). Organizational Mandate of National Identity Management. Abuja: NIMC Publications https://nimc.gov.ng/about-nimc

National Identity Management Commission. Annual Report 2023: Progress in National Identity Management. Abuja: NIMC Publications 2024.

Nigeria Data Protection Act. (2023). Federal Republic of Nigeria Official Gazette.

Nigeria Data Protection Regulation 2019. Federal Republic of Nigeria. Official Gazette Government Press.

Nigerian Correctional Service (NCoS), 'NCoS Enrolls Over 74% of Inmates into NIMC Database', 2024, https://www.corrections.gov.ng/ncos-enrolls-over-74-of-inmates-into-nimc- database/.

Okafor, J. & Ibe, P., Data protection and vulnerable populations in Nigeria: Legal frameworks and implementation challenges, Nigerian Law Journal, vol. 28, no. 2, 2022, pp. 156–173.
Owoeye, K. & Dahunsi, F., Nigeria's digital identity ecosystem: Progress, challenges, and prospects for inclusive development, Information Development, vol. 39, no. 2, 2023, pp. 245–
Privacy International, Digital identity systems and human rights: Challenges and opportunities, London: Privacy International, 2021.

Ryan Payne, Brett A. S. Martin, and Shasha Wang. 2023. Defining Biometrics with Privacy and Benefits: A Research Agenda Volume 31, Issue 4 https://doi.org/10.1177/14413582231167645

The Nigerian Correctional Service Act. 2019. Federal Republic of Nigeria. Government Press.

The West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program: Unique Identifiers to Enable Access to Human Development Services. 2023 Transformational Technologies for Human Capital.

U.S. Government Accountability Office, Prisoner Reentry: Better Data and Coordination Could Help States Understand and Address Challenges, GAO-23-105015, 2023, https://www.gao.gov/products/gao-23-105015.

Whitley, E.A., Digital Identity: Understanding the Concepts and Implications, Digital Identity Research Programme, London School of Economics and Political Science, 2018, https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/digital- identity/Digital-Identity-Understanding-the-Concepts-and-Implications.pdf

World Bank Group's. Identification for development (ID4D) making everyone count. 2016. https://worldbank.org/id4d

PART TWO

STATE POWER AND CIVIL LIBERTIES

CHAPTER 2

Data Privacy, Surveillance, and the Media: Balancing National Security and Freedom of Expression in Nigeria’s Digital Era

by

John Ogah

johngreatogah1@gmail.com
(+234)8037526788

Abstract

In Nigeria's rapidly evolving digital era, the interplay between data privacy, surveillance, and media freedom has emerged as a critical area of national and scholarly concern. With over 107 million internet users as of January 2025 and a growing dependence on digital platforms, there has been a significant expansion of the Nigerian government's surveillance capabilities, often under the pretext of national security concerns. This development, however, has raised complex ethical, legal, and democratic challenges regarding the protection of civil liberties, particularly the rights to privacy and free expression. Despite progress marked by the enactment of the Nigeria Data Protection Act (2023), enforcement remains inconsistent, and public awareness remains limited. Media practitioners and journalists are increasingly subjected to surveillance and regulatory constraints, thereby creating a climate of intimidation and self-censorship.

Nigeria's experience reflects global challenges in the balance between digital rights and state control, as seen by regulatory models like the European Union's (EU) General Data Protection Regulation (GDPR) and regulatory dilemmas in other democracies such as India and Kenya. This paper examines the implications of Nigeria's surveillance practices on data privacy and press freedom, while also evaluating the effectiveness of existing legal and institutional frameworks. It identifies critical gaps (legal clarity, oversight, transparency, redress) and explores how global best practices can guide the development of a more balanced national framework. Drawing on the analysis of existing literature, policy documents, and secondary sources, the study highlights the urgent need for transparent, rights-respecting surveillance laws and robust accountability mechanisms. The paper concludes with practical recommendations for reforming legal and institutional structures focused on safeguarding national interests while upholding Nigeria's democratic values, press freedom, and individual privacy in the digital era.

Background to the Study

Data privacy, surveillance, and media freedom are increasingly debated in Nigeria's digital era, driven by smartphones, social media, and digital services.[1] This digital evolution has heightened the government's ability, and often its interest, in monitoring digital communication, typically under the guise of national security.

This trend has been fueled by a significant increase in internet penetration across Nigeria, with over 83 million internet users recorded in 2022[2] and an estimated 107 million active internet users as of January 2025.[3] The shift raises ethical and legal concerns about balancing surveillance, media freedom, civil liberties, privacy, and digital rights in Nigeria.[4]

Legislations like the Cybercrimes Act (2015), which grants security agencies wide-ranging powers, has raised recent concerns as critics argue that the powers are prone to abuse.[5] Despite the enactment of the Nigeria Data Protection Act (NDPA) 2023, which has marked progress towards safeguarding personal data, enforcement still remains weak, with public awareness remaining low.[6] State surveillance and intimidation foster fear and self-censorship among journalists, with Nigeria ranking 122nd in the 2025 Press Freedom Index.[7]

Globally, the debate mirrors Nigeria's struggles. A high bar for privacy protection has been set by the European Union (EU)'s General Data Protection (GDPR), while countries like India and Kenya continue to grapple with similar tensions between digital rights and national interests.[5] In Nigeria, there have been recent attempts to regulate digital platforms, like the X ban in 2021, which showcased the tendency of the state to suppress dissent in the name of national security.

Therefore, this paper seeks to explore how Nigeria can effectively adopt balanced legal frameworks and establish oversight mechanisms which can protect both national security interests and citizens' rights to privacy and free expression in an increasingly connected digital ecosystem.

Problem Statement

Globally, significant attention has been drawn to data privacy, surveillance, and media freedom. While the European Union's GDPR is widely recognised as a benchmark for strong privacy safeguards, recent reports highlight growing concerns about the threat surveillance poses to press freedom in Africa.[5] In Nigeria, media advocates and scholars have analysed the increasing use of digital surveillance under the guise of national security, which has highlighted its role in constraining free expression and undermining civil liberties.[8]

The Nigeria Data Protection Commission (NDPC) acknowledges legislative advances like the NDPA, which aims to regulate data usage.[6] However, significant gaps remain in understanding how these frameworks operate in practice, especially in Nigeria's complex digital ecosystem.

While some scholarship exists, few studies directly address how surveillance and privacy affect media freedom in Nigeria, excluding key voices and weakening civic participation through fear. Much of the existing literature is either regionally broad such as Pan-African analyses of digital authoritarianism[28] or sector specific such as cybersecurity culture in institutions,[29,30] without explicitly mapping the nexus between privacy, surveillance, and press freedom. By screening out these broader or tangential studies, this paper addresses the gap by highlighting the absence of a focused inquiry into Nigeria's digital ecosystem while offering context-specific insights to guide policymakers, media professionals, and civil society towards democratic solutions.

Objectives of the Study

- To examine the nature and scope of digital surveillance practices in Nigeria and their impact on data privacy and media freedom;

- To assess the effectiveness of existing legal and institutional frameworks in safeguarding privacy and freedom of expression in Nigeria's digital ecosystem;

- To examine how global best practices can inform Nigeria's approach towards balancing national interests with digital rights and press freedom;

- To recommend evidence-based legal and institutional reforms which can help in promoting a balanced approach towards national security, data privacy, and media freedom within Nigeria's digital age.

Methodology

Using a Systematic Literature Review, the study analysed Nigerian data privacy, surveillance, and media freedom through thematic analysis of academic, legal, and policy sources.

Criteria for Selection of the Study

Criterion	Description
Relevance to Research Objectives	Only materials related to data privacy, surveillance, media freedom, and digital rights from Nigeria and global contexts were included.
Credibility of Sources	Priority was given to peer-reviewed journals, official, and reputable source materials.
Time Frame	Materials on digital surveillance and data protection published between 2013–2025.
Geographic Focus	Focus on Nigeria, with comparative studies from Kenya, India, the UK, France, and Germany included for global context.
Language	Studies and reports published in English.

Literature Review

Digital Surveillance and Data Privacy in Nigeria

In today's increasingly interconnected digital world, where information technology influences almost every aspect of daily life, there is an increasing concern about privacy and the safeguarding of personal data.[9] Nigeria has invested substantially in surveillance infrastructure, spending more than $127 million between 2014 and 2017, with allocations continuing in subsequent years.[10] These investments, however, have been marked by a lack of transparency and accountability, as evidenced by the controversial $40 million contract with Elbit Systems, an Israeli firm, to supply technology "which enables the state to intercept all internet activity and invade users' privacy at will."[11,12] The government's use of spyware from Circles and FinFisher expanded surveillance without legal safeguards, allegedly targeting opposition, journalists, and civil society without judicial oversight or public accountability.

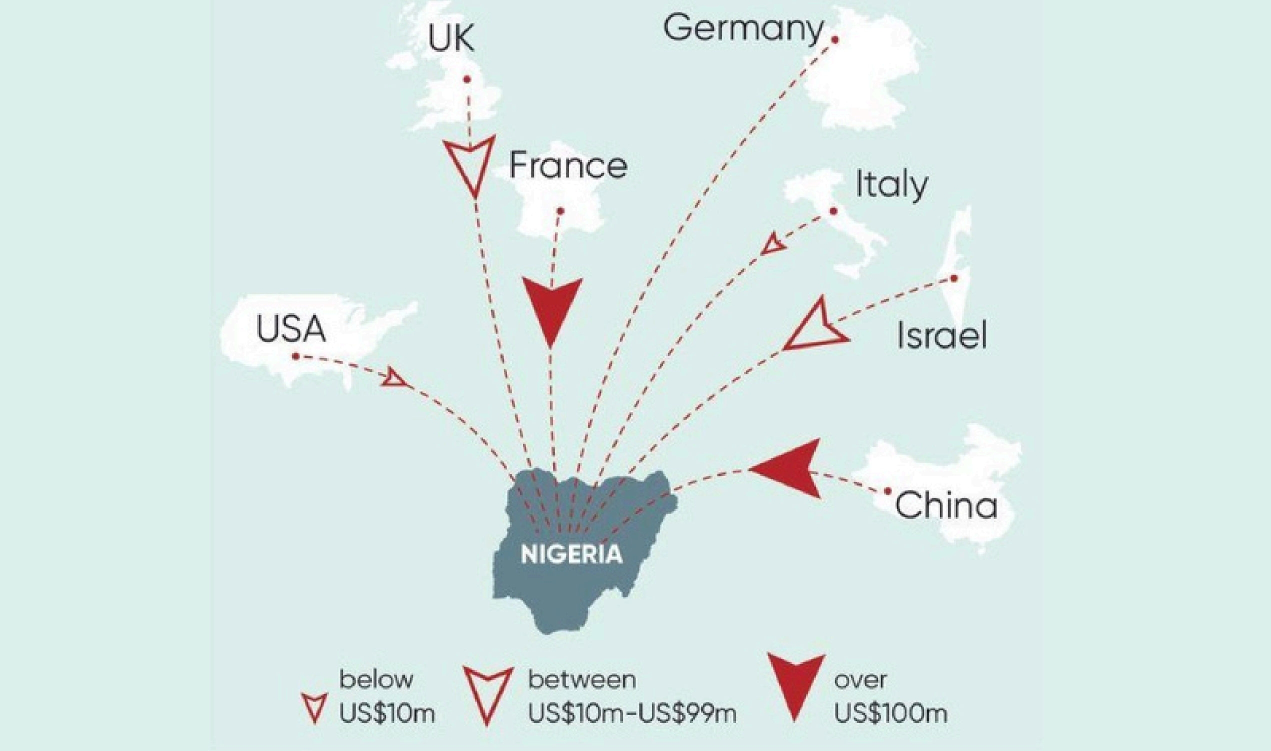
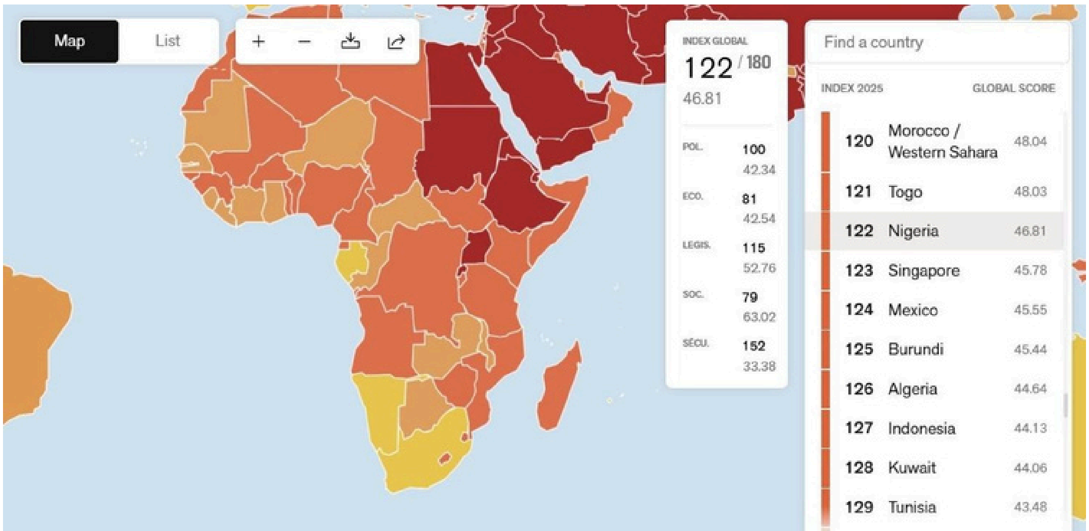


Fig. 1: Supply of surveillance technologies into Nigeria[13]

While surveillance is often justified on the grounds of national security, public safety, and counter-terrorism,[14] Nigerian laws, such as the Cybercrimes Act, the Terrorism Prevention Act, and the Lawful Interception of Communications Regulations, offer limited safeguards for digital privacy.[1] These laws, rather, provide broad powers to security agencies without crucial checks like public transparency, independent oversight, and effective judicial review.[15,16]

As noted earlier, the Nigerian government suspended X's operations in 2021, citing national security issues, a move widely seen as an attack on freedom of expression.[17-18,19] Nigeria's security agencies face criticism for unlawful surveillance and lack accountability. With declining press freedom, Nigeria ranks 122nd of 180 in the 2025 World Press Freedom Index.[7]



INDEX GLOBAL
122 / 180
46.81

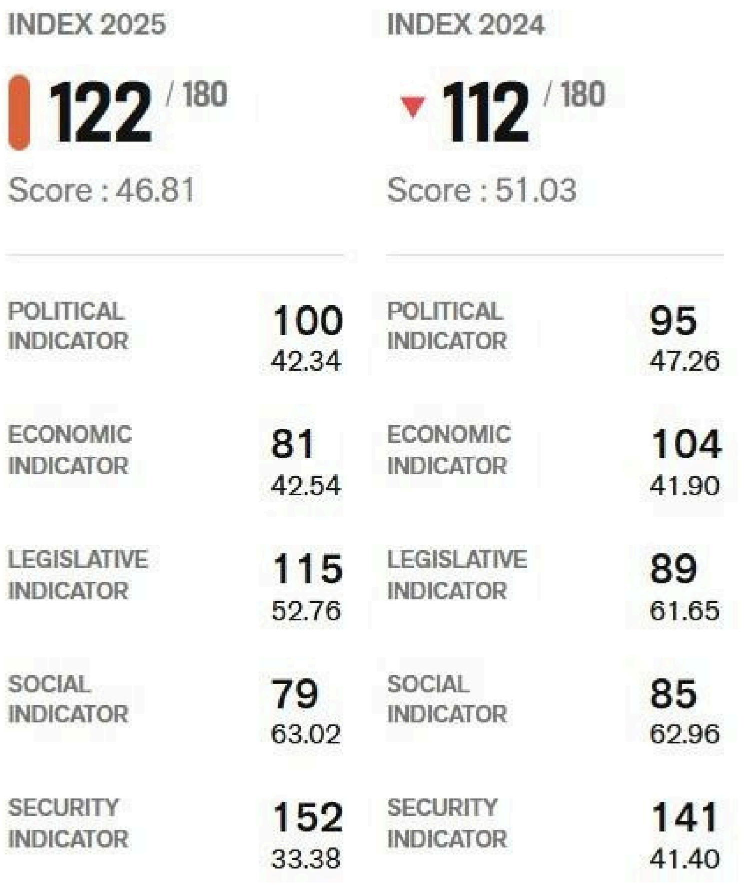
POL.	100	42.34
ECO.	81	42.54
LEGIS.	115	52.76
SOC.	79	63.02
SÉCU.	152	33.38

Find a country

INDEX 2025		GLOBAL SCORE
120	Morocco / Western Sahara	48.04
121	Togo	48.03
122	Nigeria	46.81
123	Singapore	45.78
124	Mexico	45.55
125	Burundi	45.44
126	Algeria	44.64
127	Indonesia	44.13
128	Kuwait	44.06
129	Tunisia	43.48

Fig. 2: Nigeria's Global Score on the 2025 World Press Freedom Index[20]

The use of surveillance against journalists, media office raids,[21-22,23] and arrests under cybercrime laws contribute to a hostile media environment. Constant surveillance fosters self-censorship, undermines the media's watchdog role, stifles expression, and exposes journalists using insecure tools to hack and unauthorised data access.[24] This raises pressing questions about the proportionality and legality of surveillance in a democratic society.



INDEX 2025		INDEX 2024	
122 / 180		▼ 112 / 180	
Score : 46.81		Score : 51.03	
POLITICAL INDICATOR	100 42.34	POLITICAL INDICATOR	95 47.26
ECONOMIC INDICATOR	81 42.54	ECONOMIC INDICATOR	104 41.90
LEGISLATIVE INDICATOR	115 52.76	LEGISLATIVE INDICATOR	89 61.65
SOCIAL INDICATOR	79 63.02	SOCIAL INDICATOR	85 62.96
SECURITY INDICATOR	152 33.38	SECURITY INDICATOR	141 41.40

Fig. 3: Comparative Overview of World Freedom Index Rankings for Nigeria (2024 vs. 2025)[20]

The right to privacy guarantees control over personal data and is protected by international instruments like the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR), as well as Nigeria's Constitution. However, constitutional exceptions for national security complicate enforcement amid growing surveillance, despite similar protections under regional frameworks like the European Convention on Human Rights (ECHR) and the African Charter.[25]

The Nigeria Data Protection Regulation (NDPR) of 2019,[6] and more recently, the Nigeria Data Protection Act,[26] marked a significant milestone in the establishment of a data governance framework. These laws aim to regulate the collection, processing, and storage of personal data, while aligning Nigeria more closely with global best practices such as the EU's GDPR. Nevertheless, enforcement has remained inconsistent, particularly in cases where government agencies themselves are complicit in privacy breaches.

Legal and Institutional Frameworks on Privacy and Freedom of Expression in Nigeria

Nigeria's Constitution guarantees privacy (Section 37) and expression (Section 39), but judicial interpretation is limited, with rare cases like *Emerging Market Telecommunication Services v. Barr. Godfrey Nya Eneye (2018),* affirming privacy rights.[6] The NPDA, marked a milestone in safeguarding data privacy as it mandated consent for data collection, provided individuals with the right to access, correct, or delete data, and imposed penalties for violations.[6] However, its focus on electronic data created regulatory gaps such as protection for paper-based records, with enforcement notably lacking, as evidenced by the National Information Technology Development Agency's (NITDA) failure to address violations committed by state authorities.

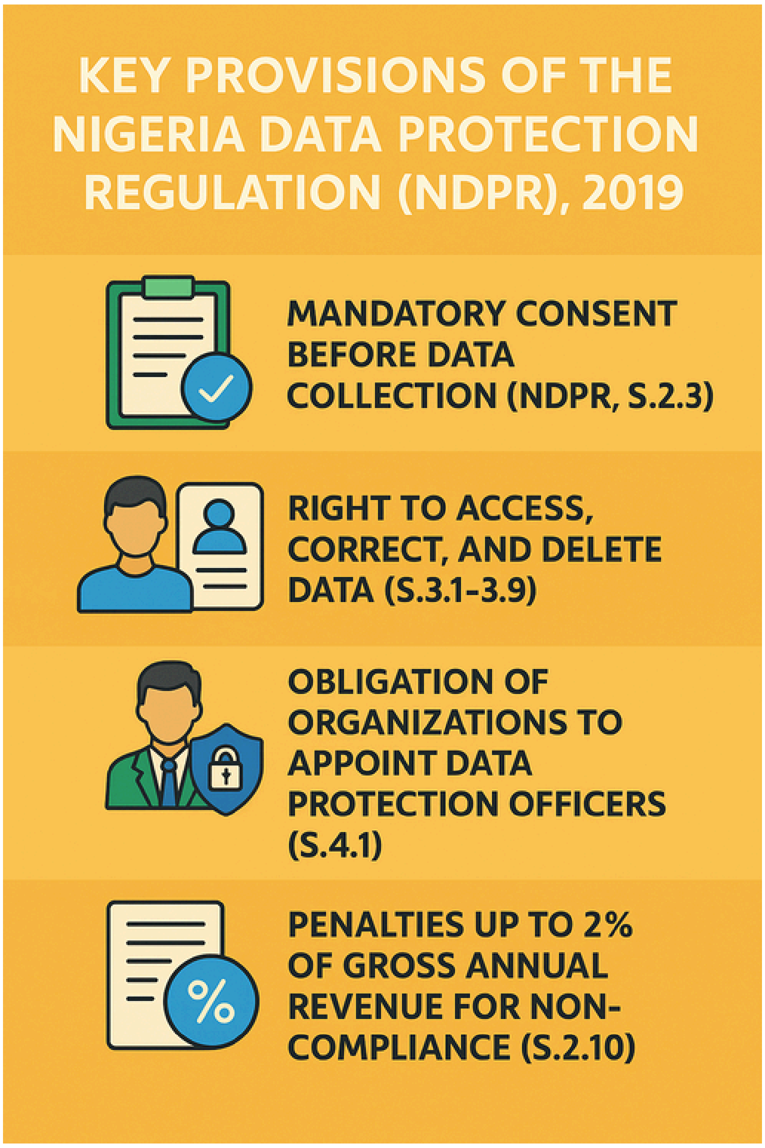

KEY PROVISIONS OF THE NIGERIA DATA PROTECTION REGULATION (NDPR), 2019
MANDATORY CONSENT BEFORE DATA COLLECTION (NDPR, S.2.3)
RIGHT TO ACCESS, CORRECT, AND DELETE DATA (S.3.1-3.9)
OBLIGATION OF ORGANIZATIONS TO APPOINT DATA PROTECTION OFFICERS (S.4.1)
%
PENALTIES UP TO 2% OF GROSS ANNUAL REVENUE FOR NON-COMPLIANCE (S.2.10)

Fig. 4: Key Provisions of the Nigeria Data Protection Regulation (NDPR)[6]

A more robust legal development came with the enactment of the Nigeria Data Protection Act (NDPA) on 14 June 2023, which replaced the NDPR. It established the Nigeria Data Protection Commission (NDPC), as an independent regulatory body, under Part II, Section 4 & 5, to regulate, license, and register high-impact data controllers/processors, and impose sanctions. The Act defines key principles under Section 24, including data minimisation, purpose limitation, and accountability. Section 40 mandates data controllers to report data breaches within 72 hours, promoting transparency.

However, Section 3(2) grants broad exemptions to security and law enforcement agencies, but only where the processing is necessary and proportionate to safeguard national interest, defence, or public safety. This provision, however, raises concerns about unchecked surveillance. The Act also requires the appointment of a Data Protection Officer "with expert knowledge of data protection law and practices, and the ability to carry out the tasks prescribed under this Act" (Section 32) while also "implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of and confident personal data in its possession..." (Section 39).

To further strengthen Nigeria's legal framework, civil society groups advocated for the Digital Rights and Freedom Bill (HB490), aimed at aligning Nigeria's laws with international digital rights standards. However, the bill was vetoed in 2019 and remains pending reconsideration. Currently, the protection of digital rights in Nigeria remains undermined by fragmented legislation, weak enforcement mechanisms, judicial conservatism, low public awareness, and rising state surveillance.

Data Presentation

Harassment of Journalists and Stifling of Dissent in Nigeria

In January 2019, armed soldiers raided the offices of Daily Trust Newspaper after it published a report on military actions against Boko Haram.[1]

During the raid, several journalists were detained, and computers were confiscated. In 2019 and 2022, four broadcast stations were fined for allegedly airing hate speech[2,3], a move widely seen as an attempt to suppress critical journalism.

Another prominent case occurred in May 2022, when Agba Jalingo, a journalist from *CrossRiverWatch*, was arrested and charged with treason and cybercrimes after exposing corruption involving the former governor of Cross River State.[4] Despite court orders for his release, he remained in detention for more than 170 days without bail.

International Comparisons: Harassment and Surveillance in Other Democracies

- **The Pegasus Spyware Controversy in India:** In July 2021, the Pegasus Project, an investigative collaboration between Amnesty International and 17 global media outlets, revealed that Pegasus spyware, developed by Isreal's NSO Group, was allegedly used by the Indian government to surveil journalists, opposition leaders, and civil society actors. A leaked database of over 50,000 phone numbers included 300 Indian contacts, such as opposition leader Rahul Gandi, political strategist Prashant Kishor, and journalists like Siddharth Varadarajan. Forensic analysis confirmed traces of Pegasus in multiple devices. India's Supreme Court condemned vague security claims, launched an inquiry, and ruled that indiscriminate surveillance violates privacy under Article 21, urging transparency after 2023 spyware attacks.[5]

- **FBI Surveillances of Journalists in the United States:** In 2021, it was revealed that the United States Department of Justice under previous administrations secretly obtained phone and email records of Journalists from The Washington Post, CNN, and The New York Times in an attempt to identify whistleblowers.[6] This revelation sparked bipartisan outrage leading to reforms to strengthen journalist protections.

- **Rwanda – Disappearances and Surveillance of Journalists:** In East Africa, the Rwandan government employed digital surveillance and repression tactics to suppress dissenting voices[7] (HRW, n.d). Journalists like John Williams Ntwali have reportedly been subjected to threats and arbitrary detention, with digital evidence indicating he was under targeted surveillance before his disappearance and eventual death[8].

Judicial Responses to Digital Surveillance

- **Okoiti v. Communications Authority Of Kenya**

  "...In January 2017, Kenya's Communications Authority (CAK) proposed a Device Management System (DMS) to monitor stolen, counterfeit, and unapproved mobile devices. The system, however, raised concerns as it would grant access to subscribers' call data and other private information. Okiya Okoiti challenged Kenya's plan to install surveillance on mobile networks, arguing it was unconstitutional, lacked public participation, and violated privacy. The government defended it as necessary to track illegal devices. The High Court found that the system was "a threat to the subscribers' privacy" and that there were less restrictive measures that could be used to identify illicit devices. The High Court ruled the system was unlawful, citing privacy jurisprudence from international and regional bodies, including the European Court and UN Human Rights Committee......"

Legal Frameworks for Data Protection: Comparative Analysis

- **United Kingdom:** The United Kingdom, post Brexit, adopted a revised version of the EU General Data Protection Regulation (GDPR), referred to as the UK GDPR, alongside the Data Protection Act (DPA) 2018. The UK GDPR reflects EU GDPR principles including lawfulness, fairness, transparency, and data minimisation, and applies to UK-based and foreign organisations handling UK residents' personal data. Public authorities and large-scale data processors must appoint a Data Protection Officer; the Information Commissioner's Office enforces compliance, and individuals have rights to access, correct, erase, and object.

- **Germany:** In Germany, the GDPR is complemented by the Federal Data Protection Act (BDSG), which came into effect on May 25, 2018, alongside the GDPR. Germany operates a decentralised system, with multiple data protection authorities operating across its 16 federal states. The BDSG lowers the requirement for appointing Data Protection Officers (DPOs) and establishes comprehensive regulations for the processing of employee data. The Act upholds the data subject rights established under the GDPR and permits supervisory authorities to impose sanctions based on the overall turnover of an entire corporate group.

- **France:** France also implements the GDPR through its updated domestic laws, notably Law No. 2018-493 and subsequent decrees. Enforcement is carried out by the Commission Nationale de l'nformatique et des Libertés (CNIL), which possesses broad investigative powers, including on-site inspections and online audits. French data subjects are entitled to GDPR-consistent rights alongside legal recourse mechanisms. Collectively, all three countries exemplify the harmonized yet locally adapted implementation of GDPR standards across Europe.[10]

Discussion of Findings

The data reveals how Nigeria's national security policies and surveillance practices intersect with declining media freedom and data privacy. Incidents like the Daily Trust Raid and Agba Jalingo's detention reflect journalist intimidation. Laws such as the Cybercrimes and Terrorism Acts are often misused to suppress press freedom. This aligns with Nigeria's 2025 World Press Freedom Index ranking of 122 out of 180, indicating worsening legal and safety conditions for journalists.

Findings further reveal that despite the enactment of the Nigeria Data Protection Act, enforcement remains weak, and public awareness, as mandated by the Act in Section 5, is low. Key sections such as Section 24 on data processing principles and Section 40 on breach notification, are undermined by Section 3(2) -- which grants broad national security exemptions without proportionality or independent oversight. The legal gap highlights civil liberties' vulnerability despite reforms, unlike GDPR countries, where institutions like ICO and CNIL ensure accountability and oversight, including for national security measures.

Okoiti and Pegasus cases show unchecked surveillance erodes trust and media freedom. Kenya's ruling aligns with Article 17 of the ICCPR and Article 8 of ECHR, exposing Nigeria's gap between Section 37 rights and surveillance practices. India's Pegasus case revealed surveillance threats to civil liberties. In Nigeria, weak oversight and broad security claims enable overreach, harming press freedom, rights, and encouraging self-censorship.

Conclusively, the findings show that Nigeria's current frameworks do not yet balance national security with democratic rights. Robust reforms like the narrowing of NDPA security exemptions, passing the Digital Rights and Freedom Bill, and empowering the NDPC with true enforcement autonomy, are essential to align Nigeria with global best practices.

Policy Recommendations

To protect digital rights while ensuring national security, Nigeria must adopt a balanced, rights-centred frameworks that uphold data privacy, regulates surveillance, and protects media freedom. Drawing from global best practices and local realities, the following recommendations are proposed:

To the Government:

- **Review Surveillance Laws:** Existing laws like the Cybercrimes Act and Terrorism Prevention Act should be revised to incorporate clear safeguards which protect against arbitrary surveillance and uphold constitutional rights;
- **Strengthen NDPC Enforcement Powers:** The Nigeria Data Protection Commission should be granted full autonomy to monitor all data handlers;
- **Pass the Digital Rights and Freedom Bill:** This Bill would safeguard digital rights, including freedom of expression, data privacy, and online liberties.

To Civil Society Organisations:

- **Enhance Judicial and Civil Oversight:** Collaborate with the judiciary by vetting surveillance for legality and democracy;
- **Promote Public Awareness:** Promote public awareness through campaigns educating communities on digital rights, data protection, and responsible online platform use.

To the Media:

- **Adopt Secure Digital Practices:** News organisations and journalists should adopt and prioritise secure digital tools;
- **Amplify Digital Rights Discussions:** The Media should actively report on surveillance and privacy violations;
- **Collaborate on Legal Reforms:** Media organisations and press unions should continually join legal reform efforts to protect expression, privacy, and press freedom in the digital space.

To Citizens:

- **Know and Defend Your Digital Rights:** Citizens should proactively learn and defend their digital rights;
- **Engage in Civic Advocacy:** Citizens should participate in digital rights advocacy, support stronger legislation, and hold officials accountable for violations of privacy or expression.

Conclusion

This research shows that despite the Nigerian Data Protection Act, surveillance continues to threaten press freedom and privacy. Weak enforcement, low public awareness, and poor judicial oversight persist. Lessons from Kenya, India, and GDPR countries stress the need for accountability, transparency, and rights-based digital governance. National security must not override constitutional and human rights; urgent legal coherence and institutional independence are essential to safeguarding Nigeria's democratic values.

To ensure that reforms are both practical and measurable, Nigeria should set clear policy benchmarks. By 2030, the country could aim to improve its World Press Freedom Index ranking from 122nd to below 100. Similarly, the Nigeria Data Protection Commission (NDPC) should publish annual enforcement reports on compliance and data breaches. Additionally, public campaigns should target raising digital rights awareness for at least 50% of Nigerian internet users before 2030. Such benchmarks give policymakers, civil society, and the media clear indicators of progress, ensuring reforms advance a democratic digital ecosystem that balances national security, privacy, press freedom, and accountability.

Data Sources for Figures

Figure 1: Supply of surveillance technologies into Nigeria: Nigeria has been revealed as Africa's largest customer of surveillance technology contracts, spending hundreds of millions of dollars annually, and at least US$2.7bn on known contracts between 2013–2022. This is the equivalent of $12 per Nigerian citizen.

Figure 2: Nigeria's Global Score on the 2025 World Press Freedom Index: Nigeria ranks 122 out of 180 countries, with a global score of 46.81. The index evaluates press freedom based on five indicators: political context, economic environment, legal framework, socio-cultural context, and safety of journalists. Nigeria scored particularly low in journalist safety (ranked 152), highlighting significant concerns about media freedom in the country.

Figure 3: Comparative Overview of World Freedom Index Rankings for Nigeria (2024 vs. 2025) (The overview illustrates the change in Nigeria's rankings and scores across five indicators: Political, Economic, Legislative, Social, and Security. Nigeria's overall ranking declined from 112th in 2024 to 122nd in 2025, with a drop in the total score from 51.03 to 46.81)

Figure 4: Key Provisions of the Nigeria Data Protection Regulation.

References

- E.A. Onatuyeh, D. Oghorodi, E.A. Okpako, E. Ojei, G. Osakwe, N.B. Chinedu, S.K. Okoh, V.C. Odu, P.U. Chinedu and W. Nwankwo, 'Cybersecurity and Business Survival in Nigeria: Building Customer's Trust', African Journal of Applied Research, 11/1 (2024), 786–813.
- Statista, 'Number of Internet Users in Nigeria from 2018 to 2022, with Forecasts from 2023 to 2027', Statista https://www.statista.com/statistics/183849/internet-users-nigeria/ [accessed 21 June 2025].
- DataReportal, 'Digital 2025: Nigeria', DataReportal https://datareportal.com/reports/digital-2025-nigeria [accessed 21 June 2025].
- G. Oyedokun, W. Babalola and W. Sakpere, 'Balancing Surveillance and Privacy: Legal Frameworks Governing Technology in the Digital Age', ResearchGate (2025), 13, 212–226 https://www.researchgate.net/publication/389986954_Balancing_Surveillance_and_Privacy_Legal_Frameworks_Governing_Technology_in_the_Digital_Age [accessed 21 June 2025].
- Amnesty International, Amnesty International Report 2020/21: The State of the World's Human Rights (London: Amnesty International, 2021) https://www.amnesty.org/en/wp-content/uploads/2021/06/English.pdf [accessed 8 July 2025].
- National Information Technology Development Agency (NITDA), Nigeria Data Protection Regulation 2019: Implementation Framework https://www.dataguidance.com/sites/default/files/ndpr_implementation_framework_november_2020.pdf?utm [accessed 1 July 2025].
- Reporters Without Borders, '2024 World Press Freedom Index – Journalism under Political Pressure', Reporters Without Borders https://rsf.org/en/2024-world-press-freedom-index-journalism-under-political-pressure [accessed 22 June 2025].
- Paradigm Initiative, LONDA Digital Rights in Africa Report (2022) https://paradigmhq.org [accessed 21 June 2025].
- Human Rights Watch (HRW), 'Q & A: US Warrantless Surveillance under Section 702 of the Foreign Intelligence Surveillance Act', Human Rights Watch (2017) https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance [accessed 10 July 2025].
- T. Ogunmokun and S. Musa, Assessing Data Protection in Nigeria: Biometric Identity, Surveillance, Encryption and Anonymity, and Cybercrimes (Tech Hive Advisory, 2022) https://cdn.prod.website-files.com/641a2c1dcea0041f8d407596/644d26941c9116d1fa3b0e8e_Accessing-Data-Protection-1.pdf [accessed 1 July 2025].
- E. Ogala, '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 1 July 2025].
- Electronic Intifada, 'Scandal in Nigeria over Israeli Arms Firm's Internet Spying Contract', Electronic Intifada https://electronicintifada.net/blogs/jimmy-johnson/scandal-nigeria-over-israeli-arms-firms-internet-spying-contract?utm [accessed 2 July 2025].
- Institute of Development Studies, 'Nigeria Spending Billions of Dollars on Harmful Surveillance of Citizens', IDS (2023) https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/ [accessed 3 July 2025].
- Nigeria Country Report, 'Surveillance Law in Africa: A Review of Six Countries', IDS OpenDocs https://opendocs.ids.ac.uk/ndownloader/files/48184975 [accessed 1 July 2025].
- T. Babatunde, 'How Nigerian Authorities Use Cybercrime Act to Silence Free Press', Punch (2024) https://punchng.com/how-nigerian-authorities-use-cybercrime-act-to-silence-free-press/?utm [accessed 2 July 2025].
- DigWatch, 'Cybercrimes (Prohibition, Prevention, etc) Act, 2015 | Nigeria', DigWatch https://dig.watch/resource/cybercrimes-prohibition-prevention-etc-act-2015-nigeria?utm [accessed 2 July 2025].
- Premium Times, 'Nigeria Lifts Twitter Suspension after Seven Months', Premium Times https://www.premiumtimesng.com/news/headlines/505531-nigeria-lifts-twitter-suspension-after-seven-months.html?tztc=1 [accessed 10 July 2025].
- Premium Times, 'Editorial: Twitter Ban in Nigeria: A Real Risk to Our Democracy', Premium Times https://www.premiumtimesng.com/news/headlines/466341-editorial-twitter-ban-in-nigeria-a-real-risk-to-our-democracy.html [accessed 10 July 2025].
- University of Pennsylvania Carey Law School (UPenn), 'The Suspension of Twitter Operations in Nigeria: Beyond Free Speech', University of Pennsylvania Carey Law School Blog https://www.law.upenn.edu/live/blogs/106-the-suspension-of-twitter-operations-in-nigeria [accessed 10 July 2025].

- [Duplicate of 7 removed to avoid repetition].
- Africanews, ‘Nigeria Army Explains Media Raid over Classified Info Publication’, Africanews (2019) https://www.africanews.com/2019/01/07/nigeria-army-explains-media-raid-over-classified-info-publication/ [accessed 8 July 2025].
- Al Jazeera, ‘Nigeria Raids Paper, Arrests Journalists over Boko Haram Coverage’, Al Jazeera (2019) https://www.aljazeera.com/news/2019/1/7/nigeria-raids-paper-arrests-journalists-over-boko-haram-coverage [accessed 8 July 2025].
- Monitor Civicus, ‘Media Freedom under Attack: Raid of Media Outlet, Several Journalists Arrested, Four Broadcasters Fined’, Civicus Monitor https://monitor.civicus.org/explore/media-freedom-under-attack-raid-media-outlet-several-journalists-arrested-four-broadcasters-fined/ [accessed 8 July 2025].
- M. Idris, O.A. Omolara, O. Omotola, A.O. Adebayo and R. Muhammad, ‘Digital Safety of Journalists in Lagos State’, Konfrontasi Journal: Culture, Economy and Social Changes, 11/3 (2024), 146–158 https://doi.org/10.33258/konfrontasi2.v11i3.306.
- M. Ibrahim, A.O. Kazeem and U.D. Dauda, ‘Right to Privacy and National Security in Nigeria: In Search of Exact Confines of Its Boundary’, Journal of Legal Studies and Research, 9/1 (2023) https://www.amofinsolicitors.com.ng/publication/right-to-privacy-and-national-security-in-nigeria-in-search-of-exact-confines-its-boundary-kazeem-a-oyinwola-esq.pdf.
- DLA Piper, ‘Data Protection Laws in Nigeria’, DLA Piper Data Protection Laws of the World https://www.dlapiperdataprotection.com/?c=NG&t=law&utm [accessed 1 July 2025].
- O. Babalola, ‘Data Protection and Privacy Challenges in Nigeria (Legal Issues)’, Mondaq (2020) https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues [accessed 3 July 2025].
- C. Achinivu, ‘The Supply of Digital Authoritarianism to Africa: An Empirical Study’, *The African Review*, 5 (2024), 525–546 https://ouci.dntb.gov.ua/en/works/96nGgdB9/.
- O.O. Oyefeso, ‘An Analysis of Cybersecurity Culture among the Nigerian Academia’, *Kontagora International Journal of Educational Research (KIJER)*, 2/2 (2025) https://doi.org/10.5281/zenodo.15103811.
- J. Garba, J. Kaur and E. Nuraihan, ‘Design of a Conceptual Framework for Cybersecurity Culture amongst Online Banking Users in Nigeria’, *Nigerian Journal of Technology*, 42/3 (2023) https://doi.org/10.4314/njt.v42i3.13.

PART THREE

TECHNOLOGY ADOPTION AND GOVERNANCE

CHAPTER 3

Rights, Context, and Inclusion in AI Design for Public Sectors in Nigeria

by

Tosin Dada

ServiceNow Business Process Analyst, DXC Technology, ServiceNow MVP, and AI enthusiast

Abstract

This paper examines the implementation of artificial intelligence systems in Nigeria's public sector through the lens of enterprise automation best practices. The broad objective is to propose a Rights-Context-Inclusion (RCI) framework to guide ethical and effective AI deployment in government services. The methodology involves drawing from experience in ServiceNow implementations and analysis of Nigeria's digital transformation initiatives to identify critical gaps in current approaches. Key findings reveal that Nigeria's rapid adoption of AI in public sector services lacks a comprehensive framework that ensures rights protection, contextual appropriateness, and inclusive access, with current implementations demonstrating a pattern of designing for technically sophisticated users while inadvertently excluding vulnerable populations.

The study identifies three critical problem areas: rights protection gaps, including insufficient attention to algorithmic transparency and consent management; contextual misalignment where AI systems designed for Western contexts fail to account for Nigeria's infrastructure constraints and cultural diversity; and exclusionary design that risks widening the digital divide. Key recommendations include establishing a National AI Ethics Council, mandating pre-deployment impact assessments, updating procurement policies, implementing open standards for bias testing, requiring multilingual interface support, and adopting phased roll-out approaches with hybrid service models. The research provides evidence-based recommendations for sustainable AI governance that balance efficiency with equity and rights protection.

Background to the Study

Nigeria's digital transformation journey has accelerated significantly with the introduction of the Strategic Roadmap and Action Plan (SRAP) 2.0 by the National Information Technology Development Agency (NITDA)[1]. The country's ambitious AI initiatives in government services represent both unprecedented opportunities and significant challenges that mirror patterns observed in enterprise automation deployments.

The Nigerian government's approach to AI implementation includes several flagship initiatives: Service-Wise GPT, which serves as a digital assistant for civil servants; healthcare AI systems under the Nigeria Digital in Health Initiative (NDHI); and tax automation systems like TaxPro Max.[2] These initiatives demonstrate Nigeria's commitment to leveraging AI for improved public service delivery. However, Nigeria's complex socio-economic landscape presents unique challenges. With only 51.6% internet penetration, significant gender gaps in mobile phone ownership (women are 23% less likely than men to own a mobile phone), and over 100 million citizens lacking formal identification, the digital divide poses substantial barriers to the implementation of inclusive AI.[3]

From an enterprise automation perspective, these challenges are familiar. ServiceNow implementations across multiple organizations have shown that technology adoption without proper change management and inclusive design often fails to achieve the intended outcomes. The same principles apply to government AI systems, but with higher stakes given the constitutional obligations to serve all citizens equitably.

Problem Statement

Nigeria's increasing adoption of AI in public sector services lacks a comprehensive framework that ensures the protection of rights, contextual appropriateness, and inclusive access. Current AI implementations demonstrate a pattern of designing for technically sophisticated users in well-connected urban areas while inadvertently excluding vulnerable populations who most need government services.

The core problem manifests in three critical areas:
Rights Protection Gaps: Despite the Nigeria Data Protection Act 2023, there is insufficient attention to algorithmic transparency, consent management, and redress mechanisms in AI system design.[4] An example is a system like Service-Wise GPT, where a consent interface that informs users in plain language about data usage and also provides clear opt-out functionality.

Contextual Misalignment: AI systems designed for Western contexts often fail to account for Nigeria's infrastructure constraints, cultural diversity (with over 250 ethnic groups and more than 500 languages), and the requirements for integrating legacy systems. For instance, digital health tools deployed in rural areas often lack offline functionality for low-bandwidth environments, while education platforms may not offer content in widely spoken Nigerian languages, thereby limiting their practical utility.

Exclusionary Design: Current AI implementations risk widening the digital divide by assuming universal digital literacy and access, potentially violating constitutional principles of equal treatment under the law. For instance, platforms such as TaxPro Max, where accessibility features are poorly implemented, highlight the need to support screen-readers and hybrid (digital and face-to-face) formats of service delivery to achieve fairness in access to all citizens. This problem is urgent because early design decisions in AI systems become embedded and difficult to change, potentially institutionalizing exclusion in the very systems meant to serve all Nigerian citizens. Once procurement cycles are set up and the system of long-term contracts with vendors is implemented, path dependencies can become established, and thus initial design errors become entrenched, and subsequent reforms become disproportionately costly and complex.

Objectives

This paper aims to examine how AI is currently being applied within Nigeria's public sector, using lessons from enterprise automation to evaluate its effectiveness, scalability, and level of governance readiness. It seeks to identify where gaps exist in rights protection, inclusive design, and equitable access, particularly regarding how AI systems affect marginalized or underrepresented groups. The broader goal is to provide evidence-based recommendations that can inform future policy decisions, technical standards, and implementation strategies consistent with Nigeria's governance priorities and digital transformation agenda.

The project will produce a set of key deliverables, including a framework of indicators to measure the performance, fairness, and inclusiveness of AI systems used in public service delivery. It will also propose policy instruments and regulatory measures suited to Nigeria's institutional context, alongside an analytical report mapping the country's AI landscape, scalability potential, governance readiness, and existing inclusion challenges.

Methodology

This study adopts qualitative documentary and comparative policy analysis, supplemented by secondary quantitative data on digital access, infrastructure, and citizens' adoption of digital systems. It aims to methodically examine the design and implementation of artificial intelligence (AI) systems across Nigeria's public sector, through the analytical framework of Rights, Context, and Inclusion (R/C/I).

The main corpus of documents consisted of government policy frameworks and government reports published between 2018 and 2025 such as: National Digital Economy Policy and Strategy (NDEPS, 2019); Nigeria Data Protection Act (NDPA, 2023); Nigeria Digital in Health Initiative (NDHI) Reports (2022 -2025); and, Publications of the Office of the Head of Civil Service regarding Service-Wise GPT (2024-2025). Similarly, complementary materials were regional and global AI governance frameworks, which include the African Union Continental Artificial Intelligence Strategy (2024), the European Union AI Act (2021), and the Recommendation on the Ethics of AI by UNESCO (2021).

As case studies, three Nigerian flagship AI-enabled systems were chosen, representing a variety in sectors: Service-wise GPT Service-based knowledge management using AI; Nigeria Digital in Health Initiative (NDHI) - health digitisation and the use of AI; and TaxPro Max, AI-based anomaly detection and revenue automation. The cases were chosen as they are some of the most widely publicised AI implementations in the public sector in Nigeria, reflect different institutional spheres, and demonstrate different implementation issues.

There are no primary surveys and interviews with citizens involved in the study, limiting the possibility of direct influence of lived experiences. Rather, the dependency on secondary data and official reports might favour state-centric accounts. These shortcomings are recognised, and the results are to be seen as indications on policy and governance levels.

Literature Review

Inclusion in Artificial Intelligence

The concept of inclusion in artificial intelligence encompasses both technical and social dimensions that are critical for equitable AI deployment. Inclusion requires deliberate design choices that ensure AI systems serve diverse populations, accommodate varying levels of digital literacy, and provide accessible interfaces across linguistic and cultural boundaries. Research demonstrates that AI systems often perpetuate existing inequalities when inclusion is not prioritized from the design phase. In the context of government services, this translates to AI systems that may inadvertently exclude citizens based on language, location, disability status, or socioeconomic factors.

The inclusive AI framework emphasizes three core principles: representational inclusion (ensuring diverse voices in AI development), distributional inclusion (equitable access to AI benefits), and procedural inclusion (meaningful participation in AI governance). These principles are particularly relevant for Nigeria's public sector, where constitutional obligations require equal treatment of all citizens regardless of their digital capabilities or geographic location.

AI Governance Frameworks

The African Union's Continental Artificial Intelligence Strategy (2024) sets the stage for regional AI governance, emphasizing the importance of aligning AI development with African values and development priorities. While it offers a strong foundation, it lacks detailed guidance tailored to individual national contexts like Nigeria.

Globally, frameworks such as the European Union's AI Act and UNESCO's Recommendation on the Ethics of AI provide robust principles for responsible AI use. However, these frameworks often assume infrastructure and institutional capacity that many developing countries, including Nigeria, are still building. As such, meaningful adaptation is required for these models to be actionable in Nigeria's public sector.

Emerging literature highlights the central role of public trust in the successful adoption of AI systems in governance. In Nigeria, electronic identity adoption surveys indicate that credibility and trust are among the most powerful predictors of citizen adoption eclipsing an exclusive focus on technical factors.[5]

The additional complementary studies have shown that trust, combined with digital literacy, has a significant positive impact on utility and acceptance of e-government platforms.[6] The systematic reviews of AI governance at global level confirm that the lack of transparency, accountability, and institutional trust is an unavoidable condition to ensure that government-driven AI systems receive the support of the population.[7] Within Nigeria's legal framework, these trust imperatives align with existing authorities: the Nigeria Data Protection Act 2023 foregrounds rights through privacy and consent provisions; the Constitution of the Federal Republic of Nigeria (1999, as amended) establishes the context by safeguarding equality and due process; and instruments such as the Freedom of Information Act (2011) and the Cybercrime Act (2015) reinforce inclusion by mandating openness, redress, and protection against digital harms. Together, these anchors provide a normative basis for embedding rights, context, and inclusion in AI governance, thereby translating trust into enforceable guarantees.

In contexts like Nigeria, where citizens often express skepticism toward government institutions, the use of AI must be accompanied by clear communication, transparency, and mechanisms for public feedback. Trust-building involves more than technical performance; it requires ethical design, accountability for decisions made by or supported through AI, and safeguards against misuse. Without these, even well-intended innovations may face public resistance or rejection.

Digital Inclusion and Government Services

Literature on digital transformation in government consistently highlights three essential success factors: user-centered design, infrastructure readiness, and strong change management. Case studies from peer countries show that AI systems, when deployed without accounting for digital literacy gaps, often perpetuate systemic exclusion, particularly among vulnerable populations. The push for "digital by default" public services has introduced efficiency gains but also unintended consequences. When not paired with accessible alternatives such as offline support or assisted digital channels, such models risk widening the very digital divide they aim to bridge by creating new forms of exclusion when not accompanied by alternative access channels and support systems.[8]

Enterprise Automation Lessons

ServiceNow's Center of Excellence model provides proven frameworks for technology governance that translate well to government AI contexts.[9] Key principles include stakeholder engagement, phased implementation, continuous monitoring, and clear escalation procedures.

Research on enterprise automation failures consistently identifies common patterns: inadequate change management, insufficient user training, poor integration with existing systems, and lack of ongoing support. These patterns are directly relevant to government AI implementations.

Nigerian Context

The Bureau of Public Service Reforms' analysis of AI-driven reforms highlight both opportunities and constraints in Nigeria's civil service context.[10] Key findings include enthusiasm for AI among senior officials, but significant capacity gaps at implementation levels.

Studies of Nigeria's digital divide reveal persistent inequalities that AI systems must address rather than exacerbate. The National Human Rights Commission's advocacy for ethical AI regulation provides important legal and constitutional context for rights-based design.[11]

AI and Public Trust

Emerging literature highlights the central role of public trust in the successful adoption of AI systems in governance. In contexts like Nigeria, where citizens often express skepticism toward government institutions, the use of AI must be accompanied by clear communication, transparency, and mechanisms for public feedback.

Trust-building involves more than technical performance; it requires ethical design, accountability for decisions made by or supported through AI, and safeguards against misuse. Without these, even well-intended innovations may face public resistance or rejection.

Capacity Building and Institutional Readiness

Multiple studies underscore that technical infrastructure alone is insufficient for AI readiness. Institutional capacity, particularly the skills, structures, and leadership commitment required to oversee AI initiatives, is just as critical. In the Nigerian public sector, there is a notable shortage of AI-literate civil servants and a lack of structured training pathways for ethical AI use. While efforts like the 3 Million Technical Talent (3MTT) program are promising, there remains a disconnect between national talent initiatives and specific public sector needs.

Data Presentation

Digital Access Statistics

Despite growing investments in digital infrastructure, 51.6% of Nigerians have internet access, reflecting a persistent national digital divide. This divide is further widened by a significant gender gap, with women being 23% less likely than men to own mobile phones, a key tool for digital participation. Identification access also remains a barrier: an estimated 100 million

Nigerians lack formal identification, limiting their ability to access digital services, financial platforms, and government programs. In terms of geography, urban areas enjoy internet penetration rates three times higher than rural regions, underscoring the unequal distribution of digital connectivity across the country.

Current AI Implementation Status

Service-Wise GPT represents the most visible success story. According to published reports, this digital assistant enables civil servants to access policies instantly, with users reporting 2-3 hours saved daily. From a business process standpoint, this initiative aligns with enterprise knowledge management challenges, where I have seen great success among power users, but adoption drops off quickly among less tech-savvy users. This innovation has seen an over 90% user satisfaction rate among its users, as stated by Dr. Folasade Yemi-Esan, Nigeria's Head of Civil Service, Abuja[12].

Healthcare AI Coverage

Healthcare AI initiatives, such as the Nigeria Digital in Health Initiative (NDHI), a flagship program launched by the Ministry of Health and Social Welfare in 2025, have digitized over 720 facilities, benefited 125 million Nigerian Citizens, and empowered 2.5 million healthcare workers. These systems work when infrastructure supports them, but fail when power or connectivity is unreliable.

Tax Automation

Tax automation systems, such as TaxPro Max, utilize rule-based automation with basic AI to cross-check filings, flag anomalies, and trigger alerts. Industry observers note the promise in reducing manual errors, but transparency remains an issue.

Infrastructure Constraints

Infrastructure remains one of the most significant barriers to effective AI implementation in Nigeria's public sector. An unreliable power supply affects over 60% of healthcare facilities,[13] disrupting service delivery and system uptime. In rural and underserved regions, limited internet bandwidth[14] makes it challenging to deploy or maintain cloud-based AI systems, particularly those that require real-time data processing. Additionally, 70% of existing government databases operate on legacy platforms[15] that lack the interoperability needed for seamless AI integration. These technical limitations are compounded by a shortage of AI-literate civil servants[16] at both federal and state levels, creating operational bottlenecks and reducing the potential impact of digital transformation efforts.

Discussion of Findings

Rights-Based Design Analysis

Current AI implementations show insufficient attention to constitutional rights protection. The Service- Wise GPT system, while successful among power users, lacks transparency mechanisms that would allow citizens to understand how AI-generated advice affects their interactions with the government.

The absence of clear consent protocols for data collection, particularly in healthcare AI systems, creates potential constitutional violations. Enterprise automation experience demonstrates that rights protection mechanisms must be built into system architecture from the beginning, not added as afterthoughts.

Contextual Design Assessment

Nigeria's AI systems demonstrate a pattern of adapting Western solutions rather than designing for local contexts. The English-only interface of Service-Wise GPT excludes speakers of Nigeria's 500+ local languages, violating principles of inclusive governance. Infrastructure adaptation remains inadequate. Healthcare AI systems that require constant connectivity fail in rural areas with unreliable power and internet access, creating a two-tier system of service quality.

Inclusion Analysis

Current implementations risk institutionalizing digital exclusion. The concentration of AI benefits among urban, educated, technically sophisticated users mirrors patterns observed in failed enterprise automation projects. The absence of hybrid service models (combining digital and in-person channels) forces citizens to choose between accessing AI-enhanced services or receiving no service at all. This violates constitutional principles of equal treatment.

Governance Gaps

Nigeria lacks comprehensive AI governance structures comparable to successful enterprise automation governance models. The absence of mandatory bias testing, impact assessments, and citizen feedback mechanisms creates accountability gaps. Procurement processes prioritize technical sophistication over contextual appropriateness, leading to vendor selection that doesn't understand Nigerian constraints and citizen needs.

Policy Recommendations

- **Establish a National AI Ethics Council:** Create an independent multi-stakeholder body to guide ethical AI use in the public sector. Modelled on enterprise Center of Excellence (CoE) structures, the council should include technical experts, legal scholars, civil society organizations, and representatives from affected communities. It would have duties such as the promulgation of binding ethical principles, the organization of sector pilots, and publishing yearly transparency reports. The Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE) in conjunction with the National Information Technology Development Agency (NITDA), will be in charge of establishing the council. Within twelve months, the council has to be legally established; two or more national AI ethics guidelines have to be published annually; eight out of ten federal ministries should be reporting compliance in two years.

- **Mandate Pre-deployment Impact Assessments:** Introduce mandatory assessments to evaluate AI systems for bias, accessibility, and inclusion before they are deployed in public services. These assessments should follow clear, enforceable criteria and be made publicly available for scrutiny.

The National Information Technology Development Agency (NITDA), through the Office of the Head of Civil Service (OHCSF) will be in charge. Hundred per cent of new AI projects will have completed a PDIA before deployment; Seventy per cent or more of non-sensitive PDIA summaries will be published; and a quantifiable decrease in high-risk issues identified before deployment will have been accomplished;

- **Require Multilingual Interface Support:** Mandate that government AI systems support at a minimum Nigeria's five major languages17, such as Hausa (over 63 million), Yoruba (over 47 million), Igbo (over 31 million), Ibibio (over 10 million), and Fulfulde (18 million), including L2 speakers. This is done to ensure that there are fair provisions of access to public services. The Federal Ministry of Information and National Orientation, and technical assistance of the Federal Ministry of Communications and Information Digital Economy (FMCIDE) will be the authority in charge. 60 per cent of citizen-facing AI services will support multiple languages in three years; a quantifiable improvement in the number of people utilizing digital services in non-English-speaking groups shall be reported; at least one accessibility audit at a national level shall be done annually;

- **Strengthen Audit and Procurement Mechanisms:** Government procurement systems must be revised to focus on inclusive and context-sensitive AI vendors and to ensure independent audit facilities. Bias testing should be tested with Nigerian-specific open standards that should be used to test the vendor, as well as audit post-deployment. AI decision logs and outputs will be reviewed by accredited third-party auditors such as universities and civil society organisations to ensure transparency and accountability. Bureau of Public Procurement (BPP) under the supervision of NITDA and the Auditor-General's Office will be in charge. Within 18 months, a revised policy on AI procurement will be implemented; half of the contracts will be rated on the basis of inclusion metrics by Year 2; by Year 2, at least ten independent audits of government AI systems will be done each year;

- **Set Realistic Training Targets and increase digital rights literacy:** Launch AI literacy and technical training for a starting cohort of 50,000 civil servants, emphasizing quality, relevance, and long-term support over rapid scale. Future expansion should be data-driven and aligned with institutional readiness. Parallel investments must enlarge digital rights literacy programmes to citizens, which are part of civic education and are taught in schools, in the media and by community-based organizations. Responsible authorities are the Office of the Head of Civil Service of the Federation (OHCSF) and the Ministry of Education in cooperation with universities. 50,000 civil servants will undergo training for over three years, at least 70 per cent will complete their competency tests; a digital rights curriculum will be incorporated into secondary schools by Year 4; a survey of citizens will show higher levels of awareness of AI-related rights and redress mechanisms;

- **Adopt a Phased Rollout Approach:** Pilot AI systems in controlled, low-risk environments within government before scaling to broader services. Lessons from enterprise automation should guide deployment, testing, and governance mechanisms. To be inclusive, hybrid service models, both online and offline, will have to be supported. Iterative improvements must be informed directly by continuous monitoring mechanisms such as structured citizen feedback mechanisms. No fewer than three AI pilots will be deployed in a controlled setting before the national deployment. Ninety per cent of AI-enabled services should retain an in-person alternative, while annual reports on citizen feedback must be published, with corrective measures clearly recorded and monitored.

Conclusion

Nigeria's approach to AI in government services stands at a critical juncture. The country's ambitious digital transformation goals are achievable, but only with frameworks that ensure rights protection, contextual appropriateness, and inclusive access from the outset.

The Rights-Context-Inclusion framework proposed in this paper draws from proven enterprise automation practices while addressing Nigeria's unique constitutional, cultural, and infrastructure contexts. The framework is not merely an ethical imperative but a practical necessity. AI systems that don't respect rights, ignore context, or exclude users ultimately fail to achieve their intended outcomes.

Key findings demonstrate that current AI implementations, while showing promise, risk institutionalizing exclusion and violating constitutional principles of equal treatment. The concentration of benefits among urban, technically sophisticated users mirrors patterns observed in failed enterprise automation projects.

The recommendations provided offer a pathway toward AI governance that strikes a balance between efficiency and equity. Success requires sustained political commitment, adequate resource allocation, and genuine engagement with affected communities throughout the design and implementation process.

Nigeria's approach to AI governance will likely influence other African countries facing similar challenges. The opportunity exists to demonstrate that developing countries can lead in the implementation of ethical AI, but only with frameworks that prioritize rights, context, and inclusion from the outset.

The time for action is now, before exclusionary design becomes embedded in the systems meant to serve all Nigerian citizens. The framework and recommendations presented here provide a starting point for that essential work.

References

- Abdulkareem, A. K., Oladimeji, K. A., Ishola, A. A., Adejumo, A., and Abdulkareem, Z. J., 'Factors influencing the adoption of electronic identity in Nigeria', JeDEM - eJournal of eDemocracy & Open Government, 16, no. 1 (2024), pp. 108–129.

- Abdulkareem, A. K., and Oladimeji, K. A., 'Cultivating the digital citizen: trust, digital literacy and e-government adoption', Transforming Government: People, Process and Policy, 18, no. 2 (2024), pp. 270–286.

- Bureau of Public Service Reforms, AI-Driven Reforms in Nigeria's Civil Service (2025), available at: https://nairametrics.com/2025/05/31/fg-to-deploy-ai-blockchain-technologies-across-nigerias-mdas-to-improve-governance/ [accessed 14 July, 2025].

- DataReportal, Digital 2025: Nigeria Report (2025), available at: https://datareportal.com/reports/digital-2025-nigeria [accessed 12 July, 2025].

- Guardian Nigeria, 'Connecting Nigeria's Underserved Communities', The Guardian, 15 March 2024, available at: https://guardian.ng/technology/connecting-nigerias-unserved-underserved-communities/ [accessed 30 June, 2025].

- Jaiyeola, T., 'Nigeria to champion AI inclusion with local language model', BusinessDay NG, 19 April 2024, available at: https://businessday.ng/technology/article/nigeria-to-champion-ai-inclusion-with-local-language-model/ [accessed 2 July, 2025].

- Lahusen, C., Maggetti, M., and Slavkovik, M., 'Trust, trustworthiness and AI governance', Scientific Reports, 14 (2024), Article 71761.

- National Human Rights Commission (NHRC), Ethical AI Regulation for Human Rights in Nigeria (2025), available at: https://thenews-chronicle.com/nhrc-pushes-for-ethical-ai-regulation-to-safeguard-human-rights-in-nigeria/ [accessed 10 July, 2025].

- National Information Technology Development Agency (NITDA), Strategic Roadmap and Action Plan (SRAP 2.0) (2024), available at: https://nitda.gov.ng/wp-content/uploads/2024/02/SRAP-2.O.pdf [accessed 5 July 2025].

- Nigeria Data Protection Commission, Nigeria Data Protection Act 2023 (2023), available at: https://ndpc.gov.ng/resources/# [accessed 4 July 2025].

- Nigeria e-Government Master Plan (2023), available at: https://fmcide.gov.ng/wp-content/uploads/2023/11/NgeGovMP.pdf [accessed 6 July 2025].

- Nigeria Launches "Service-Wise GPT" to Boost Public Service Efficiency (2024), available at: https://msmeafricaonline.com/nigeria-launches-service-wise-gpt-to-boost-public-service-efficiency/ [accessed 8 July, 2025].

- Office of the Head of Civil Service of the Federation, Service-Wise GPT Implementation Report (2024), available at: https://ohcsf.gov.ng/servicewise [accessed 1 July, 2025].

- Powering Healthcare, Nigeria Market Assessment and Roadmap (2024), available at: https://www.seforall.org/programmes/powering-healthcare-hub/seforalls-powering-healthcare-programme#:~:text=Powering%20Healthcare%20Nigeria%20Market%20Assessment [accessed 9 July 2025].

- ServiceNow Inc., Enterprise Automation Governance Framework: Best Practices Guide (2024), internal documentation.

- TheCable, 'FG launches local language model for AI development', TheCable, 20 April 2024, available at: https://www.thecable.ng/fg-launches-local-language-model-for-ai-development [accessed 11 July 2025].

- Consultancy Study on 5G:The Evolved Telecommunication Technology of the Future', Nigerian Communications Commission (2024), available at: https://www.ncc.gov.ng/sites/default/files/2024-11/Consultancy-Study-on-5G--The-Evolved-Telecommunication-Technology-of-the-Furture.pdf [accessed 7 July 2025].

- Navigating Data Challenges in Nigeria's Public Sector, Aloinett Advisors (2024), available at: https://aloinettadvisors.com/2024/09/navigating-data-challenges-in-nigerias-public-sector/ [accessed 13 July 2025].

CHAPTER 4

Beyond Business: Assessing Governmental Responses to Corporate Data Misuse - A Case Study of the Nigerian Government vs Meta Platforms Inc

by

Ajibade, Basit Olalekan
Fountain University, Osogbo
Corresponding Author: inbox.basitajibade@gmail.com

Osuolale, Olatunde Misbaudeen
Fountain University, Osogbo

Adanlawo, Aayatullah Tolulope
Faculty of Law, Ahmadu Bello University, Zaria

Abstract

This study evaluates Nigeria's recent enforcement actions against Meta Platforms Inc. (2024–2025) as a test case for data-protection implementation and digital-sovereignty claims. Using a qualitative case-study method (regulatory notices, tribunal materials, and contemporaneous press), we examine the statutory bases invoked, the procedural posture, and the institutional constraints shaping outcomes. We identify divergence in Meta's forum-specific compliance posture and draw implications for Nigeria's enforcement design (mandates, penalties, due-process safeguards). We conclude with actionable recommendations on mandate clarity, penalty calibration, and cross-border coordination to increase enforceability and reduce regulatory arbitrage.

Introduction

Meta Platforms Inc. operates Facebook, Instagram, WhatsApp, and Threads at scale in Nigeria, raising recurring questions about lawful bases for processing, consent granularity, and cross-service data sharing under Nigerian law. In 2024–2025, Nigerian authorities initiated coordinated scrutiny of Meta's consent and transparency practices, triggering proceedings that have been reported as including substantial monetary penalties (source and outcomes to be specified with primary documents). This paper situates those actions within Nigeria's evolving data-protection regime and assesses their legal footing and practical enforceability. In July 2024, Nigeria's Federal Competition and Consumer Protection Commission (FCCPC), in coordination with the newly established Nigeria Data Protection Commission (NDPC), levied a staggering US $220 million fine against Meta.[2] The authorities found that Meta had systematically engaged in abusive data practices, harvesting user data without proper consent, imposing exploitative privacy settings, and treating Nigerian users differently compared to those in other regulated jurisdictions.[2] While Meta has committed to compliance actions, the fine underscores the Nigerian government's growing willingness to challenge digital monopolies.

Nigeria's data protection ecosystem has undergone a significant transformation in recent years, reflecting a broader shift toward codifying digital rights and aligning with international privacy norms. This evolution began in earnest with the introduction of the Nigeria Data Protection Regulation (NDPR) in 2019, issued by the National Information Technology Development Agency (NITDA). The NDPR laid down foundational principles for the lawful processing of personal data. These include the necessity for informed and freely given consent, the minimisation of data collected, and robust standards for transparency and accountability[3]. It also mandated the appointment of Data Protection Officers (DPOs) for large-scale data controllers and granted individuals a suite of rights such as access to their data, rectification of errors, erasure, and data portability[4].

Violations attracted penalties of up to ₦10 million or 2% of the offending company's annual gross revenue, depending on the severity of the breach.[5,6] Building on this initial framework, the Nigerian government enacted the Nigeria Data Protection Act (NDPA) in December 2023, marking a pivotal moment in the institutionalisation of data governance.

The Act established the Nigeria Data Protection Commission (NDPC) as the country's lead data regulatory authority and expanded the lawful bases for data processing. In alignment with the European Union's General Data Protection Regulation (GDPR), the NDPA legitimised data processing under six grounds: consent, contractual necessity, legal obligation, vital interest, public interest, and legitimate interest.[7]

Despite these legislative strides, enforcement continues to face substantial hurdles. The newly empowered data protection authorities contend with limited investigatory capacity, a lack of technical infrastructure, and chronic underfunding. Also, current scholarship has largely focused on the development of data protection laws, yet little attention has been given to how geopolitical power dynamics influence corporate behaviour and regulatory effectiveness in the Global South.

Problem Statement

As digital platforms extend into emerging markets, conflicts between corporate data practices and national sovereignty have become more pronounced. While firms like Meta show compliance in well-regulated regions, they often resist enforcement in weaker jurisdictions. The 2024–2025 dispute between Nigeria and Meta highlights this disparity, raising urgent questions about the ability of Global South governments to uphold data protection norms. This study explores Nigeria's regulatory response as a lens into the broader geopolitical and structural barriers that challenge equitable digital governance worldwide.

Literature Review

The concept of digital sovereignty defined as a state's ability to control data flows and enforce its own legal standards, has become central to academic and policy debates. In Nigeria, the Meta dispute reflects an emerging assertion of this sovereignty, though still constrained by institutional and geopolitical limits. Legal reforms alone are insufficient; effective digital governance requires investment in enforcement capacity, coherent policy design, and regional collaboration.[11]

The governance of personal data has emerged as a critical issue in the digital age, especially as global technology firms expand into new markets with varying regulatory capacities. In response to growing public concern over data misuse, regions such as the European Union (EU) have established comprehensive data protection regimes like the General Data Protection Regulation (GDPR), which sets a global benchmark for user privacy and corporate accountability.[9] These frameworks emphasise consent, transparency, and fairness, placing stringent obligations on data controllers and processors. However, scholars have noted that compliance with such standards is often contingent upon the strength of local enforcement mechanisms and the geopolitical leverage of host states.[10]

Nigeria's efforts to develop a coherent data protection regime have gained momentum over the past decade. The passage of the Nigeria Data Protection Act (NDPA) in 2023 marked a significant milestone in codifying data rights and aligning national law with global norms, particularly the GDPR.[11]

While the NDPA borrows heavily from the GDPR, questions remain about its enforceability in a markedly different socio-legal context. Additionally, some studies argue that transplanting foreign legal models like the GDPR into Nigeria's regulatory landscape, without adequate adaptation, risks creating a disjuncture between law on paper and law in practice. The confrontation between Nigeria and Meta Platforms Inc. illustrates these tensions. Despite statutory reforms, enforcement challenges persist.

Nigeria's regulatory bodies, particularly the FCCPC and NDPC, have been hampered by overlapping mandates, limited technical capacity, and fragmented digital governance. Structural deficiencies in Nigeria's corporate regulatory environment have long been noted, with inconsistent enforcement identified as a major factor undermining public trust and corporate accountability.[12] Meta's resistance to Nigeria's $220 million fine in 2024, including threats to exit the market, reflects how corporations may exploit these gaps to evade full compliance.

Comparative insights from other jurisdictions further highlight Meta's divergent compliance behaviours. In Europe, where institutional oversight is robust, Meta has tended to cooperate with regulatory rulings, even when facing record-setting fines.[10] However, in countries like Nigeria, Meta has adopted a more adversarial stance, often contesting the legitimacy of local regulators and questioning the proportionality of penalties. This discrepancy reflects broader power asymmetries in global data governance, where corporate conduct is shaped by the legal maturity and geopolitical influence of the regulating state.

Global data governance remains highly fragmented, with no overarching international framework for corporate accountability in data protection. The absence of harmonised global standards allows platform companies to exploit regulatory arbitrage, adjusting compliance strategies based on jurisdictional strength.[13] An iterative, inclusive governance model, one that balances global norms with local realities, is urgently needed, as illustrated by the Nigerian case, where national regulators face powerful multinationals without adequate transnational backing.

Another dimension often overlooked in existing literature is the performative use of exit threats by technology companies when facing regulatory pushback in the Global South. Meta's behaviour in Nigeria echoes its actions in countries like India and Australia, where similar threats were employed as negotiating tools rather than definitive business strategies.[13] This raises questions about the legitimacy of corporate responses to sovereign regulation and the need for legal safeguards that prevent coercive tactics.

Overall, the literature affirms that data protection is no longer just a legal or technical matter but a deeply geopolitical issue. Nigeria's response to Meta offers a critical test case for Global South regulators. However, without stronger global coordination and domestic capacity building, these efforts risk being undermined by the structural imbalances of the global data economy.

Materials and Methods

This study employed a qualitative case study approach centred on Nigeria's regulatory actions against Meta Platforms Inc. between July 2024 and April 2025. Primary materials will comprise:

- FCCPC/NDPC notices and orders (titles, dates, reference numbers);
- Competition & Consumer Protection Tribunal filings and judgment(s) (case number, parties, date); and
- Statutory texts (FCCPA, NDPR, NDPA).

Secondary sources are limited to major wire services and peer-reviewed or institutional policy analyses. A PRISMA-style document log (annex) records each source and its analytic use. Where possible, data were cross-referenced to resolve discrepancies and establish a coherent timeline of regulatory escalation. Future iterations of this work may benefit from triangulating these findings with interviews from regulatory officials, legal practitioners, or civil society actors involved in data rights enforcement.

Discussion of Findings

Meta's Violations of the FCCPA and NDPR: A Legal Analysis

Meta's operations in Nigeria came under intense regulatory scrutiny for violating key provisions of the Federal Competition and Consumer Protection Act (FCCPA) and the Nigeria Data Protection Regulation (NDPR) - the country's foundational data protection laws. The company's data practices, particularly around consent, platform integration, and transparency, were found to contravene legal standards.

Under the FCCPA, FCCPC deemed Meta's bundling of WhatsApp data with Facebook and Instagram services without granular user consent as "unfair, deceptive, and abusive," violating Sections 114 (Right to information in plain and understandable language) and 120 (Consumer's right to cancel advance reservation, booking or order) of the Act.[14] Additionally, Meta was criticised for offering weaker privacy safeguards in Nigeria than in the EU, undermining the principle of equitable consumer protection.[2]

Meta was also found to have violated the NDPR, which mandates explicit, informed consent for each category of data processing. Instead, it used opt-out and ambiguous consent mechanisms that denied Nigerian users real control. The company also appeared non-compliant with structural NDPR requirements, such as appointing a Data Protection Officer and submitting annual audits.[8] Both the FCCPC and NITDA criticised Meta's privacy policies as overly technical and opaque, breaching the NDPR's standards for transparency and clarity.[14] Users were not clearly informed about cross-platform data sharing, particularly involving WhatsApp, rendering any presumed consent invalid. In July 2024, these violations culminated in a $220 million fine issued by the FCCPC and the Nigeria Data Protection Commission (NDPC). This landmark penalty signaled Nigeria's growing resolve to assert data sovereignty and enforce consumer protections in its digital economy.[12]

A more rigorous legal analysis of Meta's alleged violations reveals the need to engage explicitly with the statutory basis of Nigeria's enforcement actions. Under Sections 114 and 120 of the FCCPA, conduct deemed "unfair, deceptive, or abusive" was applied to Meta's bundling of services and opacity in consent structures. However, these sections were not originally tailored to digital data contexts, raising questions about the elasticity of their interpretation. Similarly, the Nigeria Data Protection Regulation (NDPR) mandates informed, explicit, and granular consent for each category of data processing, but the legal threshold for what constitutes "informed" or "freely given" consent.

Remains underdeveloped in Nigerian jurisprudence.[16] A closer reading of the NDPR and FCCPA enforcement provisions, along with Nigeria's evolving judicial interpretations, particularly in the tribunal's April 2025 ruling, clarifies whether the $220 million fine rests on a sound legal footing or was primarily a policy-driven deterrent. This sharper doctrinal engagement is essential to assessing the enforceability and credibility of Nigeria's data protection framework.

Enforcement Challenges in Meta's Violation of the FCCPA and NDPR

Nigeria's $220 million fine against Meta in July 2024 marked a strong assertion of regulatory authority. However, the case exposed key enforcement challenges when regulating powerful multinational tech firms.

One major issue was evidentiary. The FCCPC alleged WhatsApp collected 44 categories of metadata, violating the NDPR's data minimisation rule. Yet regulators lacked clear criteria for what constituted "unnecessary" data, revealing interpretive gaps in the NDPR.[15,16]

Jurisdictional ambiguity also complicated enforcement. Meta maintained that oversight belonged exclusively to the Nigeria Data.

Protection Commission (NDPC) under the Nigeria Data Protection Act 2023, while the Federal Competition and Consumer Protection Commission (FCCPC) asserted concurrent authority under Section 17(a) of the FCCPA 2018, which empowers it to prevent unfair or deceptive market conduct. Although both agencies later signed a memorandum of understanding to coordinate on digital market regulation, this overlap initially produced uncertainty over the proper forum for investigation and delayed the commencement of formal proceedings. The dispute thus reflected Meta's procedural strategy and structural gaps in Nigeria's emerging multi-agency data governance framework.[14,17] This institutional overlap delayed action.

Enforcement was also constrained by limited technical capacity. The FCCPC and NDPC relied on external consultants for digital audits, highlighting the need for long-term investment in regulatory infrastructure. [18,8]

Meta challenged the fine's procedural basis, claiming it was not given adequate notice. In April 2025, the Competition and Consumer Protection Tribunal upheld most of the decision but nullified one order due to due process concerns.[17,19] The company also challenged the proportionality of the fine, asserting that it exceeded the statutory limit tied to its Nigerian revenue. In its ruling, the tribunal upheld the penalty by referencing the seriousness and cross-border impact of the violation, as well as Meta's capacity to comply with data protection obligations. Nigerian law, however, bases penalties on domestic turnover and specified statutory maximums under Sections 48(4-6) and 49(1) of the Nigeria Data Protection Act, 2023, which limit fines to the greater of ₦10 million or 2 percent of a data controller's or processor's annual gross revenue in Nigeria. This framework contrasts with the EU's GDPR, which expressly allows penalties calculated from global turnover.[20.] Finally, fragmented oversight among the FCCPC, NDPC, NITDA, and ARCON continues to undermine regulatory coherence. Experts recommend a unified digital governance framework to improve coordination and enforcement.[21]

Meta's Exit Threats: Strategic Posturing or Legitimate Leverage?

Following the $220 million fine, Meta hinted at a possible exit from the Nigerian market, citing regulatory unpredictability, excessive penalties, and reputational risks.[22] A spokesperson warned that the FCCPC's decision "creates an untenable environment for innovation," suggesting such enforcement could deter foreign investment. Although no formal withdrawal has been filed, the rhetoric mirrors Meta's past exit threats in Kenya, India, and Australia, moves often seen as strategic bargaining tools rather than genuine intentions.

A withdrawal would carry risks for both parties. Nigeria is one of Meta's largest African markets, with millions relying on its platforms for commerce, education, and communication. A full exit could disrupt digital infrastructure and economic activity. For Meta, abandoning Nigeria would mean forfeiting a key growth market and potentially encouraging other Global South regulators to take firmer action, thus accelerating regional digital sovereignty.[21]

Regulators have warned that exit threats may be viewed as coercive attempts to undermine legal authority. Both the FCCPC and NDPC assert that no corporation is above the law. Analysts argue that rather than yielding to pressure, Nigeria should use this moment to invest in local alternatives, strengthen compliance mechanisms, and reinforce legal resilience.[20] Regardless of Meta's final decision, Nigeria's stance has already set a precedent for digital accountability across Africa.

Meta's Divergent Responses to Data Governance: Global North vs. Nigeria

Meta's approach to data governance reveals stark contrasts between its cooperative compliance in the Global North and its confrontational stance in emerging markets like Nigeria.

In the European Union, Meta has generally worked within legal frameworks, even when facing steep penalties. After being fined €1.2 billion in 2023 by Ireland's Data Protection Commission for unlawful data transfers, Meta responded by filing appeals and shifting from a "legitimate interest" basis to a consent-based model without threatening service withdrawal.[23]

Other jurisdictions show similar patterns. In Australia, Facebook initially blocked news content to protest new media compensation laws but reversed course after negotiations.[24] In India, WhatsApp threatened to leave over message-tracing mandates but ultimately remained, making limited concessions.[25] These examples suggest that exit threats often serve as leverage, not intent.

By contrast, Meta's response in Nigeria has been notably adversarial. Following the FCCPC's $220 million fine in July 2024 for exploitative consent practices and weaker data protections than those in the EU. Meta disputed the ruling and accused Nigerian regulators of misapplying data laws. WhatsApp's Nigerian privacy notice, for instance, referenced "consent" only once compared to ten times in the EU version.[26]

Instead of engaging constructively, Meta threatened to withdraw services; a move Nigerian authorities dismissed as “pressure tactics.” In April 2025, a tribunal upheld the fine, reinforcing the state’s regulatory resolve.[19]

This disparity underscores broader power asymmetries in global data governance. Meta complies procedurally in jurisdictions with robust institutional capacity but adopts a more defiant, transactional posture where regulatory enforcement is perceived as weaker. The Nigerian case raises urgent concerns about digital sovereignty, enforcement equity, and the uneven standards practised by global tech platforms.

Meta’s resistance in Nigeria should not be seen purely as a Global South compliance gap. Similar tactics such as blocking news links in Canada under the Online News Act show a broader corporate strategy of confronting regulation.

The real distinction lies in how regulatory design, institutional capacity, and civic pressure interact. In Nigeria, civil society actors like Paradigm Initiative, Media Rights Agenda, and EiE Nigeria play a crucial role in shaping these outcomes.[27]

While the analysis has thus far concentrated on state-corporate interactions, the regulatory environment in Nigeria is also shaped by non-state stakeholders whose contributions warrant recognition. Civil society organisations such as Paradigm Initiative, Media Rights Agenda, and Enough is Enough Nigeria have played an instrumental role in advocating for stronger data protection mechanisms through litigation, public awareness campaigns, and policy consultations[22]. Their interventions not only pressured regulators to act but also contributed to the public discourse that legitimised state enforcement.

Policy Recommendations

Issue	Recommendation
Regulatory coherence	The FCCPC and NDPC should, within 90 days, adopt a joint coordination protocol through a public Memorandum of Understanding like the FCCPC and NCC’s January 2025 MoU, backed by statutory regulation or executive directive, that assigns lead jurisdiction by issue, sets joint investigative procedures, and delivers single-window notices to platforms. Success should be measured by the number of joint cases resolved without duplication, shorter case timelines, and higher compliance rates, drawing on emerging models such as Digital Regulators Forums for governing domestic digital sectors.
Capacity building	Invest in NDPC: algorithmic audit expertise, DPIA tools, technical staff, and independent funding. Leverage partnerships with AU, IOM, and Mastercard.

Rights-based expansion	Amend legislation to cover profiling, automated decision-making, and data portability, especially in ad-targeting contexts.
Multilateral leverage	Develop pan-Africa coalition for data governance (e.g., ECOWAS/AU frameworks), amplifying negotiating weight.
Sustainable compliance	Rather than fines alone, require platform-in-the-loop solutions: local data storage, transparent consent processes, periodic audits, protected DPO offices.

Conclusion

Nigeria’s Meta case illustrates that credible platform enforcement turns on mandate clarity, due-process-sound orders, and penalties calibrated to verifiable statutory hooks. With coordinated FCCPC–NDPC action, transparent procedures, and turnover-sensitive penalties, Nigeria can reduce arbitrage and improve compliance. without relying on symbolic fines or unenforceable threats.

References

- 2 Reuters, 'Nigeria fines Meta Platforms $220 million for violating consumer data laws' (19 July 2024) https://www.reuters.com/
- 3 Privacy Bee for Business, 'Guide to the Nigerian Data Protection Regulation (NDPR)' https://privacybee.com/business/guide-to-ndpr/
- accessed 8 October 2025.
- 4 Tsedaqah Attorneys, 'Rights of Data Subjects and Their Enforcement under the NDPR' (Tsedaqah Attorneys, undated) https://tsedaqahattorneys.com/rights-of-data-subjects-ndpr/
- accessed 8 October 2025.
- 5 CyberPlural, 'Key Elements of NDPR' (CyberPlural Blog, undated) https://cyberplural.com/key-elements-of-ndpr/ accessed 8 October 2025.
- 6 LexpraxisNG, 'What You Need to Know About Data Compliance in Nigeria' (LexpraxisNG Blog, undated) https://lexpraxisng.com/data-compliance-in-nigeria/ accessed 8 October 2025.
- 7 Nigeria Data Protection Commission, 'About Us' (April 2025) https://ndpc.gov.ng/about-us/ accessed 8 October 2025.
- 8 PraiseGod Neeka, Biragbara Neeka and Lilian Adat, 'Data Breach in Nigeria: A Case for Local Accountability' (2025) 7 African Journal of Engineering and Environment Research 148.
- 9 Future of Privacy Forum, 'Nigeria's New Data Protection Act, Explained' (2023) https://fpf.org/ accessed 8 October 2025.
- 10 Navjot Singh and Suman Bishnoi, **'Navigating GDPR Compliance: The Intersection of Data Governance, Accountability, and Organisational Culture'** (2024) 12(4) *International Journal of Innovative Research in Engineering and Multidisciplinary Physical Sciences https://doi.org/10.37082/ijirmps.v12.i4.230875 accessed 8 October 2025.Singh, N., & Bishnoi, S. (2024). Navigating GDPR Compliance: The Intersection of Data Governance, Accountability, and OrganisationalOrganizational Culture. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 12(4). https://doi.org/10.37082/ijirmps.v12.i4.230875*
- 10 Downes, L. (2018). GDPR and the End of the Internet's Grand Bargain. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228046
- 11 Babalola, O. (2024). The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4786872
- 12 Ogbechie, C., Ogbechie, C., & Koufopoulos, D. N. (2014). *Corporate Governance Practices in Nigeria* (pp. 373–394). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-44955-0_15
- 13 Kuzio, J., Ahmadi, M. H., Kim, K. C., Migaud, M. R., Wang, Y. F., & Bullock, J. B. (2022). Building better global data governance. Data & Policy, 4, e17. https://doi.org/10.1017/dap.2022.17.
- Federal Competition and Consumer Protection Commission, Federal Competition and Consumer Protection Act 2018 (Government of Nigeria, Abuja).
- 15 AEO Law Practice. (2025). *Assessing the Competition & Consumer Protection Tribunal's Judgment in Meta Platforms Inc/WhatsApp LLC v FCCPC*. Lagos: AEO Law Practice.
- 16 NITDA, Nigeria Data Protection Regulation (NDPR), Abuja: National Information Technology Development Agency, 2019.
- 17 OOLawPractice. (2025). *Meta's Grounds for Appeal*. Lagos: OOLaw.
- 18 Vanguard. (2024, August 15). *$200m fine: Why Meta must be transparent in dealing with FG*. https://www.vanguardngr.com
- 19 Reuters. (2025, April 17). Nigerian tribunal upholds $220 million data privacy fine against Meta. https://www.reuters.com/world/africa/nigeria-meta-fine-2025-ruling.html
- 20 Tribune Online. (2025, May). *Can Meta's threat whittle down FCCPC's legal powers?*. https://tribuneonlineng.com
- 21 Tekedia. (2024). *Meta Fined $220m—What It Means for Nigeria's Tech Ecosystem*. https://www.tekedia.com
- 22 African Business. (2025, May). *Meta's Nigerian future in doubt after $280m fines*. https://www.african.business
- 23 Politico. (2023, May 22). Meta hit with record €1.2 billion GDPR fine over US data transfers. https://www.politico.eu/article/meta-facebook-gdpr-privacy-fine-record-eu/
- 24 Flew, T. (2021). Facebook v. Australia: Big Tech, News Media and the New Frontier of Platform Regulation. Media International Australia, 180(1), 85–100.
- 25 Singh, R. (2022). Digital Sovereignty and Platform Accountability in India: WhatsApp's Legal Challenge and Compliance Landscape. Indian Journal of Law and Technology, 18(2), 113–137.
- 26 Premium Times. (2024, July 19). Meta fined $220 million by the Nigerian government over privacy violations. https://www.premiumtimesng.com/news/headlines/xxx-meta-fined-nigeria-data.html
- 27Michael Dugeri, 'Big Tech, Regulation, and Nigeria's Moment of Resolve' (The Cable, 3 February 2024) https://www.thecable.ng/big-tech-regulation-and-nigerias-moment-of-resolve/ accessed 8 October 2025.