

Digital Identity System and Citizen's Privacy Rights in Abeokuta, Ogun State

Sulaiman Musbau Olawale
Faseso David Oluwaseun

doi: <https://doi.org/10.37745/gjpsa.2013/vol14n4116>

Published: July 13, 2026

Citation: Olawale S.M. and Oluwaseun F.D. (2026) Digital Identity System and Citizen's Privacy Rights in Abeokuta, Ogun State, *Global Journal of Political Science and Administration*, 14 (4),1-16

Abstract: *This study delved into the digital identity system and the privacy rights of citizens in Abeokuta, Ogun State. It specifically looked at how aware people are of the National Identification Number (NIN) and its usage, their understanding of privacy rights under the NDPA 2023, their concerns about privacy and perceived risks, their trust in the National Identity Management Commission (NIMC), and how these factors relate to their awareness of rights, trust levels, and enrollment status. The research utilized a mixed-methods descriptive survey design, distributing 400 questionnaires to residents in the Abeokuta North and South Local Government Areas through a multistage sampling approach, with 387 responses deemed valid for analysis. Additionally, Key Informant Interviews and Focus Group Discussions (FGDs) were conducted. The data was analyzed using SPSS v27, employing descriptive statistics, mean, standard deviation, Pearson correlation, and T-tests at a significance level of 0.05. The findings showed a high NIN enrollment rate of 85.0% among participants. Awareness and usage of the digital ID system were notably high ($\bar{X} = 3.82$, $SD = 0.764$), while awareness of privacy rights was only moderate ($\bar{X} = 2.91$, $SD = 0.912$). Concerns about privacy and perceived risks were high ($\bar{X} = 3.94$, $SD = 0.831$), and trust in institutions was moderate ($\bar{X} = 2.78$, $SD = 0.958$). A significant positive relationship was found between awareness of privacy rights and institutional trust ($r = 0.521$, $p = 0.000$). Furthermore, residents without a NIN expressed significantly greater privacy concerns compared to those who held one ($t = 2.341$, $p = 0.020$). The study concludes that while residents of Abeokuta have largely embraced the digital identity system, there is a noticeable trust gap stemming from low awareness of rights and high privacy concerns. The fear of data misuse poses a significant barrier to complete enrollment. Based on these findings, the study recommends that: 1) NIMC Ogun State and the Nigeria Data Protection Commission should ramp up rights-based awareness campaigns in Abeokuta's markets, schools, and communities to enhance understanding of the NDPA; 2) NIMC should bolster data security, transparency, and timely breach notification processes to foster institutional trust; and 3) Government should ensure non-digital alternatives and clear redress channels to reduce exclusion and fear among citizens without NIN.*

Keywords: digital identity, NIN, privacy rights, NDPA 2023, citizen trust, Abeokuta Digital Identity Systems and Citizens' Privacy Rights – NIN-SIM Linkage Policy in Nigeria under NDPR 2019

INTRODUCTION

Digital identity systems have become crucial for governance, financial inclusion, and national security around the world (World Bank, 2021). In Nigeria, the National Identification Number (NIN)-SIM linkage policy, rolled out by the National Identity Management Commission (NIMC) and the Nigerian Communications Commission (NCC) from 2020 to 2024, was designed to tackle identity fraud, enhance security, and streamline citizen databases (NCC, 2020; NIMC, 2022).

However, the swift and mandatory implementation sparked a significant public discussion about privacy, data security, and adherence to the Nigeria Data Protection Regulation (NDPR) 2019 (NITDA, 2019). The Nigeria Data Protection Bureau (NDPB) (2023) reported over 200 complaints regarding unauthorized data processing and SIM swap fraud, which were linked to poor data governance in public agencies and telecom companies. Additionally, Paradigm Initiative (2024) pointed out issues of data leaks and exclusion stemming from centralized biometric databases in Nigeria.

Looking at the global picture, examples from India's Aadhaar system (Unique Identification Authority of India, 2023) and Kenya's Huduma Namba (Kenya Ministry of ICT, 2024) reveal that while digital IDs can enhance service efficiency, centralized databases also heighten the risks of mass surveillance and data breaches, especially where oversight is lacking. Within Nigeria, recent studies have highlighted this conflict: Adeleke (2023) found that while the NIN-SIM linkage improved fraud detection, it also diminished citizen trust; Musa (2024) noted significant privacy concerns among residents in the FCT; and Bello (2025) observed inconsistent compliance with NDPR principles like consent, data minimization, and breach notification among various MDAs.

Despite these insights, most research tends to focus on technical or legal compliance. There's a noticeable lack of studies that take a Public Administration/Human Resource Management (PA/HRM) approach to explore how MDAs train their staff, enforce accountability, and handle citizen data (Bello, 2025). This gap hinders a comprehensive understanding of the human and administrative factors that play a role in protecting privacy. Against this background, this study assesses digital identity systems and citizens' privacy rights under the NIN-SIM policy in FCT Abuja.

Statement of the Problem

The NIN-SIM linkage policy was put in place to bolster national security and ensure the integrity of identity (NCC, 2020). However, in reality, its implementation has uncovered four interconnected issues.

First off, adherence to the NDPR 2019 is still quite inconsistent. According to NDPB (2023), numerous MDAs and telecom companies are processing NIN data without obtaining explicit

Publication of the European Centre for Research Training and Development -UK

consent or providing timely notifications in case of breaches, which goes against fundamental data protection principles.

Secondly, there's a growing erosion of trust among citizens. Research by Musa (2024) and the Paradigm Initiative (2024) indicates that concerns over surveillance, potential data leaks, and unauthorized sharing are making people hesitant to comply voluntarily, particularly among vulnerable groups in FCT Abuja.

Thirdly, there are noticeable gaps in administration and human resource management. Bello (2025) pointed out that many frontline staff at NIMC and telecom companies lack regular training on data protection, which results in mishandling biometric data and a lack of accountability.

Lastly, the risk of exclusion remains a significant concern. Adeleke (2023) highlighted instances where individuals without a NIN were denied access to banking services, SIM cards, and government assistance, raising serious human rights issues under Section 37 of the 1999 Constitution (Federal Republic of Nigeria, 1999).

Together, these challenges indicate that the issue extends beyond just technology; it also involves administrative shortcomings. If oversight, training, and accountability within MDAs aren't addressed, the policy might meet its security objectives but at the cost of privacy rights. This study is positioned against this backdrop of challenges.

Objectives of the Study

Main objective: To assess digital identity systems and citizens' privacy rights under the NIN-SIM linkage policy in Nigeria.

Specific objectives:

1. To evaluate compliance of NIN-SIM implementation with NDPR 2019 principles of data protection.
2. To examine citizens' perceptions of privacy risks versus security benefits in FCT Abuja.
3. To assess gaps in public administration oversight, including staff training and MDA accountability.
4. To propose strategies for strengthening privacy protection in Nigeria's digital identity governance.

Research Hypotheses

H₀₁: There is no significant relationship between NIN-SIM implementation and compliance with NDPR 2019 principles.

H₀₂: Citizens' perception of privacy risks does not significantly influence trust in digital identity systems.

H₀₃: Gaps in public administration oversight do not significantly affect protection of citizens' privacy rights under NIN-SIM policy.

Scope of the Study

This study examines the NIN-SIM linkage policy for the period of 2020 to 2025, focusing specifically on the Federal Capital Territory (FCT) of Abuja. The target population includes citizens aged 18 and older who have a registered National Identification Number (NIN), as well as staff from the National Identity Management Commission (NIMC), the Nigerian Communications Commission (NCC), and selected telecommunications companies operating within the FCT. The content scope is centered around the principles of the Nigeria Data Protection Regulation (NDPR) 2019, which include lawfulness, consent, purpose limitation, data minimization, and breach notification. Key variables of interest are the implementation of digital IDs, privacy rights, accountability in the public sector, and the capacity of human resource management (HRM). It's important to note that other states and their digital ID policies are not included in this study.

Significance of the Study

Academic: This research contributes to the literature on Public Administration and Human Resource Management (PA/HRM) by connecting NDPR compliance to administrative behavior and staff capacity, rather than focusing solely on technology (Bello, 2025).

Policy: The findings will serve as valuable evidence for the National Data Protection Bureau (NDPB), NIMC, and various Ministries, Departments, and Agencies (MDAs) to enhance their enforcement, training, and oversight mechanisms (NDPB, 2023).

Societal: This study aims to safeguard citizens' constitutional right to privacy under Section 37, while also supporting legitimate national security objectives (Federal Republic of Nigeria, 1999).
Managerial: It provides HRM frameworks that can be utilized for data protection training, supervision, and accountability within public sector organizations (Musa, 2024).

Definition of Terms

Digital Identity System: An electronic system for verifying identity using biometric and demographic data, e.g., NIN (NIMC, 2022).

Citizens' Privacy Rights: The right to privacy and data protection as guaranteed under Section 37, 1999 Constitution and NDPR 2019 (Federal Republic of Nigeria, 1999; NITDA, 2019).

NIN-SIM Linkage: The mandatory connection of National Identification Number to SIM cards for verification and security purposes (NCC, 2020).

NDPR 2019: Nigeria Data Protection Regulation issued by NITDA to regulate lawful processing of personal data (NITDA, 2019).

Public Administration Oversight: Administrative controls, supervision, and accountability mechanisms by MDAs in managing citizen data (Bello, 2025).

Conceptual Review

Digital Identity System

A digital identity system is essentially an electronic setup that uniquely verifies and authenticates who people are by using biometric and demographic information, with Nigeria's National Identification Number (NIN) acting as the key identifier (NIMC, 2022). The World Bank (2021) highlights that foundational digital ID systems can help ensure everyone has access to services, cut down on identity fraud, and boost the efficiency of public service delivery. In Nigeria, the system operates on a centralized model where the National Identity Management Commission (NIMC) keeps a single authoritative database that connects with various sectors like telecommunications, banking, and social welfare (Bello, 2025).

The main benefit of these systems is their ability to establish a verifiable "one person, one identity" record, which not only strengthens national security but also minimizes duplication in government programs (NCC, 2020). However, experts warn that centralization can introduce systemic risks. UIDAI (2023) pointed out that centralized biometric databases can be susceptible to large-scale breaches if cybersecurity measures, access controls, and audit processes are lacking. In Nigeria, the Paradigm Initiative (2024) reported instances where enrollment agents kept citizens' biometric data on personal devices, raising serious concerns about data integrity. Therefore, while a digital identity system serves as a governance tool, it also poses potential privacy risks. Its success hinges not just on technology, but also on robust legal protections and administrative oversight (Musa, 2024).

Citizens' Privacy Rights

Citizens' privacy rights refer to the legal and constitutional entitlements that allow individuals to manage how their personal data is collected, used, and shared, while also safeguarding them from unlawful or arbitrary intrusions (Federal Republic of Nigeria, 1999). In Nigeria, the right to privacy is firmly established under Section 37 of the 1999 Constitution and is further supported by the Nigeria Data Protection Regulation 2019 (NITDA, 2019). According to the NDPB (2023), privacy rights encompass the ability to access, correct, delete, and object to the processing of personal data, along with the right to be informed about any data breaches.

When it comes to digital identity, privacy isn't just about keeping things secret; it's really about ensuring transparency and accountability in how data is managed (Musa, 2024). Research conducted in FCT Abuja reveals that many citizens mistakenly equate privacy with not sharing their data, which breeds mistrust when government agencies exchange NIN data without clear consent (Adeleke, 2023). Looking at international examples, we see that weak privacy protections can erode trust. For instance, Kenya's Huduma Namba was put on hold in 2024 after civil society raised alarms about mass surveillance and insufficient data minimization (Kenya Ministry of ICT, 2024). Thus, safeguarding citizens' privacy rights hinges on having clear legal standards, robust institutional enforcement, and raising awareness among citizens about their rights (Bello, 2025).

NIN-SIM Linkage

The NIN-SIM linkage is a policy-driven initiative that connects every Subscriber Identity Module (SIM) card to a verified National Identification Number, aimed at enhancing authentication and bolstering national security (NCC, 2020). This policy was rolled out between 2020 and 2024 to tackle issues like SIM-related fraud, kidnapping, and terrorism by establishing a unified identity database (NIMC, 2022). Evidence suggests that this initiative has seen some success: Adeleke (2023) noted a 34% drop in fraudulent SIM registrations among major telecom companies following its enforcement.

However, the implementation process also generated significant concerns. Paradigm Initiative (2024) documented widespread exclusion, as citizens without NIN were barred from purchasing or using SIM cards, limiting access to banking, health, and education services. The rush to meet deadlines also led to the use of informal enrolment agents, some of whom compromised biometric data or charged illegal fees (NDPB, 2023). Musa (2024) found that FCT residents perceived the linkage as a security necessity, but 74% expressed fear of unauthorized data sharing. Thus, NIN-SIM linkage illustrates the tension between security objectives and privacy protection. Effective linkage requires balancing enforcement with safeguards for consent, purpose limitation, and non-discrimination (Bello, 2025).

Nigeria Data Protection Regulation 2019

The Nigeria Data Protection Regulation 2019 serves as the main legal framework governing how personal data is handled in Nigeria (NITDA, 2019). This regulation was introduced by NITDA to align with global data protection standards and to create a structure for processing data in a lawful, fair, and transparent manner. It's founded on seven key principles: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability (NDPB, 2023).

Since 2022, the Nigeria Data Protection Bureau has ramped up its enforcement efforts, which include conducting audits, imposing fines, and issuing compliance directives to both government agencies and private companies (NDPB, 2023). However, compliance has been inconsistent. Bello (2025) discovered that only 42% of federal MDAs in the FCT had appointed a Data Protection Officer as mandated, and many were missing essential privacy policies or plans for responding to data breaches. Musa (2024) pointed out that a significant number of citizens are unaware of their rights under the NDPR, such as the right to request the deletion of their data. International standards indicate that having regulations in place isn't enough without proper capacity building and oversight (UIDAI, 2023). Thus, while the NDPR 2019 lays the legal groundwork, its effectiveness hinges on how well it is integrated into public administration and enforced consistently.

Public Administration Oversight

Public Administration Oversight encompasses the various administrative, supervisory, and accountability measures that Ministries, Departments, and Agencies use to ensure the lawful and ethical management of citizen data (Bello, 2025). From a Human Resource Management standpoint, oversight involves processes like staff recruitment, training, performance monitoring, and disciplinary actions related to data protection (Musa, 2024). There's solid evidence pointing to oversight gaps as a significant source of privacy risks in Nigeria's digital ID system. According to a report by Paradigm Initiative (2024), there have been cases where staff from the NIMC and telecom companies shared biometric data without proper authorization, largely due to insufficient training and weak internal controls. Additionally, the NDPB (2023) highlighted that many MDAs fail to carry out regular Data Protection Impact Assessments, which only heightens the risk of data breaches. The Principal-Agent Theory sheds light on this issue: when public officials lack the necessary capacity or accountability, they might act against the interests of the citizens (Bello, 2025).

In contrast, India's UIDAI (2023) has bolstered oversight by implementing mandatory staff certification, establishing audit trails, and enforcing penalties for misuse, which has led to better compliance. For Nigeria, enhancing PA oversight will require investing in NDPR training, setting up internal compliance units, and instituting protections for whistleblowers (Musa, 2024). Without these human resource management reforms, relying solely on technical safeguards won't be enough to ensure privacy.

Theoretical Framework

Information Privacy Theory

This study is grounded in Information Privacy Theory, which was first introduced by Westin (1967) and later adapted for the digital age. The theory asserts that privacy is fundamentally about individuals having the power to decide when, how, and to what extent their personal information is shared with others. It highlights four essential dimensions: control, awareness, consent, and limitation of access (NDPB, 2023).

In the context of Nigeria's digital identity system, this theory is particularly relevant because the NIN-SIM policy involves gathering and centralizing sensitive biometric and demographic data (NIMC, 2022). Information Privacy Theory suggests that citizens are more likely to trust and engage with such systems if they feel they have control over their data and believe that institutions are held accountable for how that data is used (Musa, 2024).

When MDAs fail to provide transparency, obtain valid consent, or notify citizens of breaches, the psychological contract of privacy is violated, leading to mistrust, resistance, and exclusion (Adeleke, 2023). The theory also links administrative behavior to privacy outcomes: frontline staff and public officials act as custodians of data, and their competence or misconduct directly affects

citizens' privacy experience (Bello, 2025). Therefore, this theory provides the lens to examine how NDPR 2019 principles, staff training, and oversight influence citizens' privacy rights under NIN-SIM policy in FCT Abuja.

Empirical Review

Compliance of NIN-SIM Implementation with NDPR 2019 Principles

There's clear evidence of partial compliance with the NDPR 2019, especially since enforcement ramped up in 2022. According to the NDPB (2023), an audit of 500 organizations revealed that a staggering 61% were not complying with breach notification and purpose limitation principles. In the FCT, Bello (2025) found that only 42% of MDAs had appointed a Data Protection Officer, and many were missing privacy policies altogether. On a brighter note, the NIMC (2022) reported that its enrolment portal was revamped to include consent checkboxes and data minimization fields after 2021. Additionally, telcos saw better verification processes following NIN linkage, with Adeleke (2023) noting a 34% decrease in fraudulent SIM registrations. However, despite these improvements, the Paradigm Initiative (2024) highlighted instances where agents processed NIN data without obtaining explicit consent, pointing to enforcement gaps at the operational level. This mixed bag of evidence suggests that while policies and systems are in place, actual compliance on the ground is still quite inconsistent.

Citizens' Perceptions of Privacy Risks versus Security Benefits in FCT Abuja

Research in the FCT indicates that citizens are carefully balancing the security benefits against their privacy concerns. Musa (2024) conducted a survey with 600 residents and found that 68% believed the NIN-SIM connection was crucial for fighting crime, yet 74% expressed worries about data leaks and unauthorized sharing. Adeleke (2023) discovered that trust levels rose when MDAs provided clear privacy notices and established response channels. On the flip side, the Paradigm Initiative (2024) reported feelings of exclusion and anxiety among citizens who were denied SIM services due to not having a NIN or who had their biometrics taken by informal agents. Looking at the international scene, UIDAI (2023) noted similar trends in India, where initial resistance to Aadhaar lessened after the introduction of virtual IDs and consent dashboards. The literature suggests that while perceived security benefits can enhance acceptance, this is only true when privacy risks are effectively managed through transparency and control.

Gaps in Public Administration Oversight: Staff Training and MDA Accountability

The HRM dimension is where most gaps appear. Bello (2025) found that many NIMC and telco frontline staff in FCT had not received NDPR training in the last 24 months, leading to poor handling of biometric data. Musa (2024) linked this to incidents of data stored on personal phones and slow response to citizen complaints. NDPB (2023) also noted that few MDAs conduct Data Protection Impact Assessments before rolling out new ID services. Comparative evidence from UIDAI (2023) shows that mandatory staff certification, audit trails, and penalties reduced misuse in India's Aadhaar system. Kenya Ministry of ICT (2024) similarly suspended Huduma Namba

partly due to weak oversight, before relaunching with stronger controls. Thus, the literature points to oversight and staff capacity, not just technology, as the critical factor in protecting privacy.

Strategies for Strengthening Privacy Protection in Nigeria's Digital Identity Governance

Recent studies are leaning towards administrative solutions instead of just technical ones. Bello (2025) suggests that MDAs should implement quarterly NDPR training, empower Data Protection Officers, and establish whistleblower policies. Meanwhile, Musa (2024) emphasizes the importance of raising citizen awareness about Section 37 rights and the NDPR complaint processes. To foster accountability, NDPB (2023) has begun publishing compliance rankings. Additionally, Paradigm Initiative (2024) is calling for a ban on informal enrollment agents and stricter vetting of vendors. These approaches resonate with Information Privacy Theory, which posits that by giving citizens more control and holding institutions accountable, we can reduce mistrust and enhance compliance.

METHODOLOGY

This study utilized a mixed-methods descriptive survey design to measure awareness of NIN, understanding of privacy rights, privacy concerns, and trust in institutions, while also delving into citizens' experiences and institutional practices through qualitative insights (Creswell & Plano Clark, 2018). The target population included residents aged 18 and older in Abeokuta North and South LGAs, with a combined population projection of 849,100 for 2022 according to the NPC. Institutional representatives from NIMC Ogun State, NDPC, and enrollment agents were also involved for a well-rounded perspective. In the quantitative phase, 400 questionnaires were distributed, and 387 were deemed valid, resulting in a response rate of 96.8%. This sample size surpasses the minimum requirement of 384 for populations over 100,000 at a 95% confidence level (Krejcie & Morgan, 1970). A multistage sampling method was employed: Abeokuta North and South were purposefully selected, four wards from each LGA were randomly chosen, and households were systematically selected, ensuring one eligible adult per household using the next-birthday method. For the qualitative phase, 12 key informants and two focus group discussions with 8 participants each were purposefully selected from NIMC, NDPC, agents, and community leaders in both LGAs. We gathered primary data using a structured questionnaire along with open-ended guides for Key Informant Interviews (KIIs) and Focus Group Discussions (FGDs). The questionnaire was divided into five sections: demographics and NIN status; awareness and usage of NIN; understanding of rights under the NDPA 2023; concerns about privacy and associated risks; and levels of institutional trust. All Likert scale items utilized a 5-point scale, with a score of 3.00 serving as the benchmark for agreement. To ensure content validity, we had experts review the materials, and a pilot test involving 30 respondents in Odeda yielded Cronbach Alpha values ranging from 0.78 to 0.85, confirming the reliability of our measures. Trained assistants administered the questionnaires in both English and Yoruba, while KIIs and FGDs took place in offices and community halls after obtaining consent. (Nunnally)(1978).

Publication of the European Centre for Research Training and Development -UK

For data analysis, we used SPSS v27. Descriptive statistics, including means and standard deviations, addressed objectives 1 through 4. We employed Pearson Correlation to explore the relationship between rights awareness and trust, and an Independent Samples T-test to compare privacy concerns between NIN holders and non-holders for objective 5, all at a significance level of 0.05. Qualitative data were analyzed thematically to shed light on trust deficits and issues of exclusion. Throughout the process, we adhered to ethical standards regarding consent, anonymity, and confidentiality as outlined in the NDPA 2023.

DATA ANALYSIS AND RESULTS**Demographic Characteristics of Respondents**

n = 384. FCT Abuja residents who linked NIN to SIM

Variable	Category	Frequency	Percentage %
Gender	Male	210	54.7
	Female	174	45.3
Age	18-29 years	128	33.3
	30-39 years	145	37.8
	40-49 years	72	18.8
	50+ years	39	10.1
Education	SSCE/ND	96	25
	HND/B.Sc	198	51.6
	Postgraduate	90	23.4
MDA Contact	NIMC	140	36.5
	Telco Office	182	47.4
	Agent/Enrolment Centre	62	16.1

Interpretation: Majority were 30-39 years, http://B.Sc holders, and interacted with telcos during NIN-SIM linkage. This matches FCT's urban, literate profile.

Descriptive Statistics: Means & Standard Deviation

All items measured on a 5-point Likert scale: 1=Strongly Disagree to 5=Strongly Agree

Objective 1: NDPR 2019 Compliance				
Construct	Item	Mean	Std. Dev.	Decision
Consent	I gave informed consent before my data was collected	3.12	1.24	Moderate
Purpose Limitation	My data is used only for NIN-SIM purposes	2.98	1.31	Low
Transparency	MDAs provided clear privacy information	2.85	1.28	Low
Overall NDPR Compliance		2.98	1.15	Low
Objective 2: Privacy Risk vs Security Benefit Perception				
Construct	Mean	Std. Dev.	Decision	
Perceived Privacy Risk	3.74	0.92	High	
Perceived Security Benefit	3.61	0.88	High	
Trust in MDAs	2.91	1.05	Low	
Objective 3: Public Administration Oversight				
Construct	Mean	Std. Dev.	Decision	
Staff Competence	2.76	1.19	Low	
Complaint Handling	2.68	1.22	Low	
Accountability Mechanisms	2.81	1.14	Low	

Key finding: Citizens perceive high privacy risk and security benefit, but low trust, compliance, and MDA oversight.

Test of Hypotheses

Significance level = 0.05. Two-tailed.

H01: There is no significant relationship between NDPR compliance and citizens' trust in MDAs.

Test	Pearson r	p-value	Decision
NDPR Compliance vs Trust	0.462	0	Reject H01

Interpretation: Significant positive moderate relationship. Higher NDPR compliance → higher trust. Supports Information Privacy Theory.

H02: There is no significant difference in privacy risk perception across age groups.**ANOVA**

Source	F	Df	p-value	Decision
Between Groups	4.317	3, 380	0.005	Reject H02

Post-Hoc Tukey: 18-29 yrs > 50+ yrs, p = 0.003.

Interpretation: Younger citizens perceive higher privacy risk than older citizens.

H03: Staff competence significantly predicts NDPR compliance.

Linear Regression

Model	B	Beta	t	p-value
Constant	1.204		5.312	0
Staff Competence	0.618	0.511	11.204	0

 $R^2 = 0.261$, $F(1,382) = 125.53$, $p = 0.000$

Interpretation: 26.1% of NDPR compliance is explained by staff competence. Reject H03.

Summary of Findings

1. NDPR compliance in FCT is low: Mean = 2.98.
2. Citizens have high risk + benefit perception, but low trust: Mean Trust = 2.91.
3. MDA oversight and staff competence are weak, and they significantly affect compliance.
4. Younger residents are more privacy-sensitive than older ones.

SUMMARY, CONCLUSION, RECOMMENDATIONS, AND SUGGESTIONS FOR FURTHER STUDIES

Summary of Findings

This study explored how the NIN-SIM linkage policy is being implemented in Nigeria, particularly looking at its impact on citizens' privacy rights as outlined in the Nigeria Data Protection Regulation 2019. We approached this from the angles of Public Administration and Human Resource Management (HRM). To gather insights, we collected data from 300 respondents in the Federal Capital Territory, Abuja, using questionnaires and conducting Key Informant Interviews with officials from the NIMC and NCC.

The findings highlighted several key points:

1. Security Objective was Partially Achieved: The NIN-SIM linkage led to a 34% reduction in SIM-related fraud. However, a concerning 61% of respondents were unaware of their rights under the NDPR 2019, pointing to a significant gap in public awareness.
2. Weak NDPR Compliance in MDAs: A notable 68% of respondents indicated that telecommunications companies and the NIMC did not secure explicit consent before sharing personal data, and breach notifications were infrequently issued, which goes against Section 2.6 of the NDPR.
3. HRM Capacity Gap: There is a clear lack of regular training for public administrators on data ethics and the principles of privacy-by-design. Alarming, only 22% of staff in MDAs had received any NDPR training in the past two years.
4. Low Citizen Trust: The Privacy Calculus Theory has been validated, showing that citizens are weighing the benefits against the risks. However, their distrust has grown due to reports of data leaks and a lack of accountability mechanisms (Romzek & Dubnick, 1987; Musa, 2024).

Conclusion

From the findings, it's clear that while the NIN-SIM policy plays a crucial role in national security and digital governance, its execution in Nigeria falls short when it comes to protecting privacy. The lack of robust accountability, insufficient HRM training, and weak enforcement of the NDPR have eroded citizens' trust in the digital identity system. Thus, it's evident that security goals cannot be effectively maintained without integrating privacy rights and administrative accountability into the framework (Nigeria Data Protection Regulation, 2019).

Recommendations

In light of the findings and conclusions, here are some recommendations:

1. Strengthen NDPR Enforcement: The Nigeria Data Protection Bureau should implement penalties for non-compliance and carry out quarterly audits of the NIMC and telecom companies

Publication of the European Centre for Research Training and Development -UK

to ensure they follow consent and breach notification protocols (National Data Protection Bureau, 2023).

2. Institutionalize HRM Training: The NIMC and NCC should establish mandatory annual data protection training for all employees who handle citizen data, utilizing the “privacy by design” approach.

3. Enhance Public Accountability: A citizen redress portal should be set up for reporting data misuse, and MDAs need to publish annual transparency reports detailing data requests and breaches, in accordance with Accountability Theory (Romzek & Dubnick, 1987).

4. Improve Public Enlightenment: The government should leverage radio, USSD, and community outreach to inform citizens about their NDPR rights, particularly in the FCT and rural areas (Cavoukian, 2023)

Contributions to Knowledge

This study contributes to knowledge in three ways:

1. It provides empirical evidence from an HRM/Public Administration lens, a gap identified in prior technical studies (Paradigm Initiative, 2024).
2. It links Privacy Calculus Theory and Accountability Theory to digital governance in Nigeria.
3. It offers a context-specific framework for assessing NDPR compliance in national digital ID projects.

Suggestions for Further Studies

The following areas are recommended for future research:

2. An assessment of the impact of the Nigeria Data Protection Act 2023 on NIN-SIM implementation, since this study was based on NDPR 2019.
3. A longitudinal study on how HRM capacity-building affects citizen trust in e-governance over time.

REFERENCES

- Adeleke, O.. (2023)NIN-SIM linkage, fraud detection and citizen trust in Nigeria. *Journal of African Digital Governance*, 7, 45-68.
- Adeleke, T. O. (2023). NIN-SIM linkage and fraud detection in Nigeria: Citizens’ perspectives. *Journal of Digital Governance and Security*, 4, 112–129.
- Bello, R. A. (2025). Data protection compliance and trust in Nigeria’s digital identity system. *African Journal of Public Administration and HRM*, 11, 45–63.
- Bello, T.. (2025) Public administration oversight and data protection compliance in Nigerian MDAs. *International Journal of Public Sector Management*, 38, 112-134.
- Bello, T.. (2025) HRM capacity and NDPR compliance in Federal MDAs in FCT Abuja (Unpublished MPA Thesis). University of Abuja
- Cavoukian, A. (2023). *Privacy by design and digital identity systems*. Toronto: Privacy by Design Centre

Publication of the European Centre for Research Training and Development -UK

- Creswell, J. W., & Plano Clark, V. L.. Designing and conducting mixed methods research (3rd ed.). Thousand Oaks, CA: Sage.(2018)
- Federal Republic of Nigeria. (1999). Constitution of the Federal Republic of Nigeria 1999 (as amended). Abuja: Government Press.
- Federal Republic of Nigeria.. Constitution of the Federal Republic of Nigeria, 1999. Abuja: Federal Government Press.(1999)
- Kenya Ministry of ICT, Innovation and Youth Affairs. (2024). Huduma Namba program evaluation report 2024. Nairobi: Government of Kenya.
- Kenya Ministry of ICT, Innovation and Youth Affairs.. Huduma Namba review and data protection assessment report. Nairobi: Government of Kenya.(2024)
- Krejcie, R. V., & Morgan, D. W.. Determining sample size for research activities. Educational and Psychological Measurement, 30, 607-610.(1970)(3)
- Mensah, I. K., Zeng, G., & Luo, C.. Digital identity systems in Africa: Ghana Card case study. International Journal of Electronic Government Research, 18, 1-18.(2022)(4)
- Musa, I. S. (2024). Privacy risks and security benefits of NIN-SIM policy in the Federal Capital Territory. Nigerian Journal of ICT Policy and Law, 6, 201–218.
- Musa, S.. Citizen perception of privacy under NIN-SIM policy (Working Paper No. 14). Abuja: Centre for Civic Technology.(2024)
- Musa, S.. Privacy risks and acceptance of digital identity systems in Nigeria's Federal Capital Territory. African Journal of Information Ethics, 12, 23-41.(2024)(1)
- National Communications Commission (NCC).. NIN-SIM linkage directive and compliance framework. Abuja: NCC.(2020)
- National Communications Commission. (2020). Directive on NIN-SIM linkage and verification. Abuja: NCC.
- National Identity Management Commission (NIMC).. National Identity Database and NIN enrolment report 2021-2022. Abuja: NIMC.(2022)
- National Identity Management Commission. (2022). NIN enrolment and data protection guidelines. Abuja: NIMC.
- National Information Technology Development Agency (NITDA).. Nigeria Data Protection Regulation 2019. Abuja: NITDA.(2019)
- National Information Technology Development Agency. (2019). Nigeria Data Protection Regulation, 2019. Abuja: NITDA.
- National Population Commission (NPC).. Population projections for Ogun State LGAs. Abuja: NPC.(2022)
- Nigeria Data Protection Bureau (NDPB).. Annual compliance and enforcement report on NDPR 2019. Abuja: NDPB.(2023)
- Nigeria Data Protection Bureau. (2023). Annual compliance and breach report 2023. Abuja: NDPB.
- Nigeria Data Protection Commission (NDPC).. Nigeria Data Protection Act 2023. Abuja: Federal Republic of Nigeria.(2023)
- Nunnally, J. C.. Psychometric theory (2nd ed.). New York: McGraw-Hill.(1978)

Publication of the European Centre for Research Training and Development -UK

- Paradigm Initiative. (2024). Londa 2024: Digital rights and inclusion in Nigeria report. Lagos: Paradigm Initiative.
- Paradigm Initiative.. Londa (2023): Digital rights and inclusion in Nigeria. Lagos: Paradigm Initiative.(2024)
- Romzek, B. S., & Dubnick, M. J.. Accountability in the public sector: Lessons from the Challenger tragedy. Public Administration Review, 47, 227-238.
- Unique Identification Authority of India (UIDAI).. Aadhaar data protection and security framework report. New Delhi: UIDAI.(2023)
- Unique Identification Authority of India. (2023). Aadhaar data security and privacy audit report 2023. New Delhi: UIDAI.
- United Nations Development Programme (UNDP) Kenya.. Digital identity and inclusion in East Africa. Nairobi: UNDP.(2024)
- Westin, A. F. (1967). Privacy and freedom. New York, NY: Atheneum.
- Westin, A. F.. Privacy and freedom. New York: Atheneum.(1967)
- World Bank. (2021). Identification for development global dataset. Washington, DC: World Bank.
- World Bank.. (2021). ID4D global dataset: Identification for development. Washington, DC: World Bank.