

**ENFORCING DATA PRIVACY IN THE DIGITAL AGE: CHALLENGES AND PROSPECTS IN
NIGERIA**

NNEJI CHILOTAM VERA

GOU/U21/LAW/346

**FACULTY OF LAW,
GODFREY OKOYE UNIVERSITY,
ENUGU**

JULY, 2026



Edit with WPS Office

**ENFORCING DATA PRIVACY IN THE DIGITAL AGE: CHALLENGES AND PROSPECTS IN
NIGERIA**

BY:

NNEJI CHILOTAM VERA

GOU/U21/LAW/346

**A LONG ESSAY SUBMITTED TO THE FACULTY OF LAW, GODFREY OKOYE
UNIVERSITY, ENUGU STATE, NIGERIA, IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAW (LL. B) OF
GODFREY OKOYE UNIVERSITY, ENUGU STATE, NIGERIA.**

JULY, 2026

DECLARATION

I hereby declare that this project titled "enforcing data privacy in the digital age: challenges and prospects in Nigeria" is a product of an original research work conducted by me. All resources and references used in the preparation of this project have been duly acknowledged and cited in accordance with academic standards.

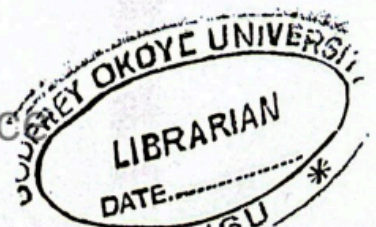
I affirm that this project has not been submitted in part or in whole to any other institution for academic award.



NNEJI CHILOTAM VERA

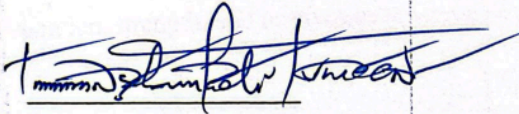
14 / 07 / 2026

DATE



CERTIFICATION

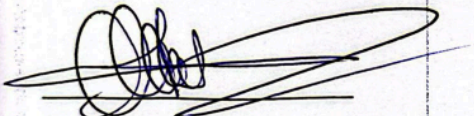
This is to certify that this study titled 'Enforcing data privacy in the digital age: challenges and prospects in Nigeria' was carried out by Nneji Chilotam Vera under our supervision and that the essay has not been submitted for the award of any degree in this or any other university.



Rev. Dr. Victor Munachimusoaga Nzebunachi
Supervisor

10/7/2026

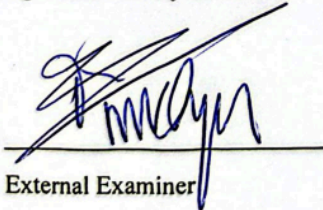
Date



Dr. G. O. Omeh
Ag. Dean, Faculty of Law

21-07-2026

Date



External Examiner

22/07/2026

Date

DEDICATION

This work is dedicated to Almighty God for His grace, guidance, and strength throughout the course of my studies.

And to my ever-loving parents and dearest siblings whose immeasurable love, unwavering faith in me, countless sacrifices, and constant prayers have been my greatest source of inspiration, strength, and motivation throughout this academic journey.



ACKNOWLEDGEMENTS

I wish to express my profound gratitude to Almighty God for granting me the strength, wisdom, and perseverance required to successfully complete this project.

My sincere appreciation goes to my project supervisor, Rev. Dr. Victor Munacimsoaga Nzebunachi, whose invaluable guidance, encouragement, and constructive criticism greatly contributed to the successful completion of this work. I am deeply grateful for the patience, dedication, and commitment shown in directing and supervising this research.

I also express my heartfelt appreciation to the Faculty of Law and all my lecturers for their dedication to teaching and for providing the academic foundation upon which this project was built. I am especially grateful to Dr. Aneke, Professor B. O. Okere, Miss Florence, the Late Rev. Fr. Somadina, Associate Professor Ajibo, and Dr. Nkolo for their invaluable contributions to my legal education and intellectual development.

I am profoundly grateful to Barrister Dr. Agidi, under whose guidance I had the privilege of undertaking my internship for four years. The practical knowledge, mentorship, exposure, and professional values I gained during this period have greatly enriched my legal education and contributed significantly to my personal and professional growth.

I equally appreciate my colleagues and friends, especially Bembe, Kosi, Amaka, Princess, Chinonso, Ogechi, Excel, Rev.sister Vivian, Ezugo, and Maxwell, for their cooperation, motivation, encouragement, and assistance in various ways during the course of this research.

My deepest gratitude goes to my beloved parents, Mr. and Mrs. Nelson Nneji, whose unwavering love, sacrifices, prayers, encouragement, and financial support made this achievement possible. I am equally grateful to my dear siblings, Marvellous and Chinemerem, for their love, understanding, and constant encouragement. Your steadfast support has been a constant source of strength and inspiration.

To everyone who contributed, directly or indirectly, to the successful completion of this project, I say a heartfelt thank you. May Almighty God richly bless and reward you all.



TABLE OF CONTENTS

Cover page-----	i
Title page -----	ii
Declaration -----	iii
Certification-----	iv
Dedication -----	v
Acknowledgements-----	vi
Table of Contents -----	vii
Table of statutes -----	xi
Table of cases -----	xiv
List of Abbreviations -----	xv
Abstract -----	xvii
CHAPTER ONE: INTRODUCTION -----	1
Background of the Study -----	1
Statement of the Problem -----	4
Research Question -----	6
Aims and Objectives of the Research -----	7
Research Methodology -----	7



Scope of the Study -----	8
Significance of the Study -----	8
Literature Review -----	9
CHAPTER TWO: CONCEPTUAL AND THEORETICAL FRAMEWORK-	15
2.1 Conceptual Framework -----	15
2.1.1 Defining Data -----	15
2.1.2 Defining Data Privacy -----	18
2.1.3 Context of the Digital Age: Technology, Data, and Society -----	21
2.1.4 Types of Data Privacy Breaches -----	24
2.1.5 Defining Enforcement, Challenges, And Prospects -----	26
2.1.5.1 Enforcement -----	26
2.1.5.2 Challenges-----	27
2.1.5.3 Prospects -----	29
2.2 Theoretical Framework-----	30
2.2.1 Privacy Protection Theories-----	30
2.2.1.1 Right to Privacy Theory -----	30
2.2.1.2 Control Theory of Privacy-----	31
2.2.1.3 Contextual Integrity Theory of Privacy -----	31
2.2.1.4 The Panoptic Surveillance Theory -----	32
2.2.1.5 The Human Dignity Theory of Privacy -----	33
2.2.2 Theories of the rule of law and compliance -----	33
2.2.2.1 Deterrence theory -----	33
2.2.2.2 Rational Choice Theory -----	34
2.2.2.3 The Institutional Theory of Enforcement -----	35

2.2.2.4 The Rule of Law Theory	35
--------------------------------------	----

CHAPTER THREE: LEGAL AND INSTITUTIONAL FRAMEWORK FOR DATA PRIVACY IN

NIGERIA	37
---------------	----

3.1 Overview of Nigeria's Legal Regime on Data Privacy	37
3.2 The Nigeria Data Protection Act 2023 (NDPA) and Subsidiary Instruments ----	39
3.3 Other Relevant Laws and Regulations	42
3.3.1 The 1999 Constitution of the Federal Republic of Nigeria as amended ----	42
3.3.2 Cybercrimes (Prohibition, Prevention, etc.) Act 2015	43
3.3.3 Child Rights Act of 2003.....	44
3.3.4 The Credit Reporting Act 2017	45
3.3.5 The Freedom of Information Act 2011	46
3.3.6 The National Identity Management Commission (NIMC) Act of 2007	47
3.3.7 Sector-specific laws on data privacy	47
3.3.7.1 Nigerian Communications Act	47
3.3.7.2 Regulatory frameworks issued by the Central Bank of Nigeria	48
3.3.7.3 National Health Act 2014.....	49
3.3.7.4 HIV/AIDS (anti-discrimination) Act 2014.....	50
3.4 Comparative Analysis: EU-GDPR and South Africa's POPIA	52
3.5 Regional Data Protection Frameworks: the ECOWAS supplementary Act and the African Union Malabo Convention.	56
3.6 Enforcement Mechanisms and Institutional Roles	59

CHAPTER FOUR: CHALLENGES AND PROSPECTS OF ENFORCING DATA PRIVACY IN

NIGERIA.....	61
--------------	----

4.1 challenges of Enforcing Data Privacy.....	61
---	----

4.1.1 Institutional and Regulatory Weaknesses	61
4.1.2 Technological and Infrastructure Constraints	63
4.1.3 Jurisdictional and Cross-Border Data Issues.....	65
4.1.4 Socio-Cultural Attitudes toward Privacy	66
4.1.5 Judicial Uncertainty and Inconsistent Remedies	68
4.2 Prospects for Effective Enforcement.....	69
4.2.1 Strengthening Legal Institutions	70
4.2.2 Enhancing Public Awareness and Digital Literacy.....	71
4.2.3 Leveraging Technology for Data Protection.....	71
4.2.4 Regional and International Cooperation.....	71
CHAPTER FIVE: SUMMARY OF FINDINGS, RECOMMENDATIONS, AND CONCLUSION---	
.....	73
5.1 Summary of Findings	73
5.2 Recommendations.....	74
5.3 Conclusion.....	BIBLIOGRAPHY
.....	77

TABLE OF STATUTES

National Statutes

Constitution of the Federal Republic of Nigeria 1999 (as amended),
section 37 2, 36, 51

section 39.....	2,
section 45.....	2
Nigeria Data Protection Act 2023,	
section 25	39
sections 26, 65	38–39
sections34–38	39
section 41	39–40
section 48	39
section 61	40
section 65	15–16
Nigeria Data Protection Regulation 2019,	
Part I (Definition of Personal Data)	16
Cybercrimes (Prohibition, Prevention, etc.) Act 2015	
section38(5)	43
section 33.....	43
Section 38	35
Central Bank of Nigeria (CBN) Consumer protection Framework, 2016	
part iv	36
Nigerian Communications Commission (NCC) Consumer code of practice Regulations 2007	
section35.....	36
Freedom of Information Act 2011,	
sections 14, 14(2)	45

section 16..... 45

Credit Reporting Act 2017

section 7(2) 44

section 6(1) 44

section 9(1) 44

Child's Rights Act 2003

section 142(9) 43

section 205(1) 43

section 205(2) 44

National Identity Management Commission Act 2007

section 26 45

Sections 16(a)– (c) 45

HIV/AIDS (Anti-Discrimination) Act in 2014

Section 13(1) 48

Section 11..... 49

National Health Act, 2014

Sections 26 and 29 48

International and Regional Statutes and Instruments

Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR),

article 4 16

article 5..... 50–51

article 19..... 53

article 45-46 53

article 83 (5) 53

article 63-65	54
Protection of Personal Information Act 4 of 2013 (South Africa) (POPIA)	
Section 4	50–51
Section 4(1)(b)	53
Section 72	53
Section 100	54
African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014	
	13
ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010)	
article 22	55
ECOWAS Supplementary Act A/SA.1/01/07 Relating to ICT Harmonisation	
.....	General Reference

TABLE OF CASES

<i>Digital Rights Lawyers Initiative v National Identity Management Commission</i> FHC/ABJ/CS/105/2021 (FHC, 22 March 2022) -----	31
<i>El-Rufai v Senate of the National Assembly</i> (2016) 1 NWLR (Pt 1494) 534 ----- 40	
<i>National Identity Management Commission v Owonikoko</i> ----- 3-4	
<i>Nwali v Ebonyi State Independent Electoral Commission (EBSIEC)</i> (2014) LPELR- 23682(CA) -----	41
<i>Ransome-Kuti v Attorney-General of the Federation</i> (1985) 2 NWLR (Pt 6) 211 (SC) -----	65–66
<i>Abacha v Fawehinmi</i> (2000) 6 NWLR (Pt 660) 228 -----	56
<i>Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo</i> (2001) 7 NWLR (Pt 711) 206 -----	18
<i>Emerging Markets Telecommunication Services Ltd v Eneye</i> (2018) LPELR-43706(SC) -----	67



LIST OF ABBREVIATIONS

AfCFTA	African Continental Free Trade Area
AU	African Union
BVN	Bank Verification Number
CBN	Central Bank of Nigeria
CSO	Civil Society Organization
ECOWAS	Economic Community of West African States
EU	European Union
FHC	Federal High Court
GDPR	General Data Protection Regulation
GAID	General Application and Implementation Directive
GPEN	Global Privacy Enforcement Network

GPA	Global Privacy Assembly
ICT	Information and Communication Technology
NDPA	Nigeria Data Protection Act
NDPC	Nigeria Data Protection Commission
NDPR	Nigeria Data Protection Regulation
NIMC	National Identity Management Commission
NIN	National Identification Number
NITDA	National Information Technology Development Agency
NCC	Nigerian Communications Commission
OECD	Organisation for Economic Co-operation and Development
POPIA	Protection of Personal Information Act
SC	Supreme Court
SIM	Subscriber Identity Module
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development



ABSTRACT

Enforcing data privacy laws in Nigeria has become a major roadblock in the modern digital era. In today's era, from banking to online shopping, all the activities demand to share personal information, and tech companies and government bodies have huge repositories of personal information. This means that normal people are highly susceptible to identity theft, leaks and unauthorized tracking. While privacy is a right of all people, the current pace of technological development and cross-border data tracking is continually threatening personal security. To be able to unravel this problem, it is necessary to examine the Nigerian laws and legislation, and examine how data protection is handled in Europe and south Africa and point out the gap. While the launch of the NDPA2023 was good, implementation is lagging because there are some structural problems that need to be addressed. They involve regulatory conflicts in which various government departments have overlapping regulations, poorly resourced agencies with no technical tools, untrained lawyers in digital forensics, and the public's lack of understanding, together with a cloud dilemma, making it difficult to track data across borders. To fix the digital economy and to restore public trust, the NDPC needs to be fully free from external interference, mandates from multiple agencies need to be streamlined and merged, judicial training needs to be improved, and public awareness needs to be raised in the grassroots, while forging alliances with foreign versions of the NDPC to monitor data trans-border transference. If the institutions which are supposed to hold violators accountable are weak, then writing the law is useless.



CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Digital technologies have greatly increased how people communicate, conduct business, and participate in society worldwide that is in virtually every aspect of modern society. In 2000, the estimated population of internet users was 400 million people worldwide. By 2019, the figure increased to over 4 billion people who use the internet.¹ It shows further that the report expanded in 2024 includes 5.3 billion people, which reveals that about 66 percent of the global population now has internet access.² Despite the opportunities this growth created, issues relating to the misuse and security of private records have emerged.³

The United Nations Human Rights Council (UNHRC) stated that people's rights should be guaranteed in the digital space as it is exercised physically in view of the rising challenges. It was first emphasized in the 2012 Resolution, while the 2021 Resolution reinforced the position to address new digital challenges such as mass monitoring, improper use of data, and privacy violations.⁴ These developments are important when

¹ THISDAY Newspapers, "Active Data Internet Subscribers Hit 142m as GSM Subscriptions Maintain Market

Lead" (20 March 2025) *THISDAY* [https://www.thisdaylive.com/2025/03/20/active-data-internet-subscribers-hit-](https://www.thisdaylive.com/2025/03/20/active-data-internet-subscribers-hit-142m-as-gsm-subscriptions-maintain-market-lead)

[142m-as-gsm-subscriptions-maintain-market-lead](https://www.thisdaylive.com/2025/03/20/active-data-internet-subscribers-hit-142m-as-gsm-subscriptions-maintain-market-lead). last accessed 30 August 2025.

² Data Reportal (Kepios), *Digital 2024: Global Internet Use Accelerates* (2024) Data Reportal <https://datareportal.com/reports/digital-2024-global-overview-report>. 30 August 2025.

³ World Bank, *World Development Report 2021: Data for Better Lives* (World Bank 2021); GSMA, *The State of*

Mobile Internet Connectivity 2023

⁴ UN Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet* UN Doc

A/HRC/RES/20/8 (29 June 2012); UN Human Rights Council, *The Right to Privacy in the Digital Age* UN Doc



assessing data protection issues in Nigeria.

Recently Nigeria has witnessed a rise in internet use in modern era. Data from Nigerian Communications Commission shows that about 142.16 million persons are active subscribers in Nigeria as of January 2025.⁵ For communication, government services, business, and social interaction, digital platforms are now used. This development contributed to economic growth but also has increased the risk improper use of private information and unauthorized surveillance.⁶

The Constitution of the Federal Republic of Nigeria (1999, as amended) protects the rights to private life. Section 37 secures protection communications between people while Section 39 protects expressive freedom and access to knowledge.⁷ The provisions of the constitution are closely linked because when privacy is violated, it can also limit their ability to freely express themselves and it may negatively affect the press.⁸ However, governments often attempt to balance right to privacy with national security and business interests, sometimes can weaken coverage accorded to sensitive details of a person.⁹

Biometric application systems in Nigeria like the introduction of Bank Verification Number (BVN) in 2014, biometric data requirement for voter registration, driver's licenses, and passport applications have led to large scale collection of personal information which has contributed to the concerns over data privacy although they were

HRC/47/L.22 (2021).

⁵ Nigerian Communications Commission, *Subscriber Statistics Report* (January 2025).

⁶ United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2021* (UNCTAD 2021).

⁷ Constitution of the Federal Republic of Nigeria 1999 (as amended) section 37 and section 39

⁸ Ibid section 37 and section 39

⁹ Ibid section 45

created to improve security.¹⁰ “According to report in 2018 was criticized for mandatory SIM card registration and inadequate data protection framework.¹¹

These weaknesses became evident during the introduction of Nigeria’s digital identity system in 2018. The system did not have strong privacy protections, making personal information easy to access which led to a legal action, in *National Identity Management Commission v Owonikoko*,¹² the Federal High Court ordered that the system be suspended until adequate protection laws were introduced because privacy is a fundamental right of the aggrieved parties.¹³ The expansion of fintech, electronic commerce, social media, and artificial intelligence has further increased the gathering of sensitive information of individuals by both government and individual owned organizations. Data breaches, phishing attacks, unauthorized sharing of data, and misuse of personal information are now common. These problems are made worse by low public awareness, limited digital literacy, and weak institutions. Personal data has grown into a valuable asset, used in targeting advertisements and behavioral analysis.¹⁴

To address these issues, Nigeria Data Protection Act was enacted in 2023. While this law aligns Nigeria with international standards, enforcement continues to be ineffective

¹⁰ Bank Verification Number (Central Bank of Nigeria website)

<https://www.cbn.gov.ng/PaymentsSystem/BVN.html> accessed 25 January 2026 at 7:20pm.

¹¹ Privacy International and Paradigm Initiative, *A State of Surveillance: Government Surveillance in Nigeria* (2018).

¹² (unreported)

¹³ New Telegraph, *NIN-SIM Linkage: Addressing Data Privacy Concerns*, 2019.

<https://newtelegraphng.com/nin-sim-linkage-addressing-data-privacy-concerns>. Last accessed 1 September 2025.

¹⁴ Organization for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2020*

(OECD Publishing 2020) ch 6 <https://www.oecd.org/digital/digital-economy-outlook-2020-3f7b7e58-en.htm>, last

accessed 25 January 2026



owing to limited resources, weak technical capacity, and difficulties regulating foreign companies.¹⁵ Compared to jurisdictions such as the European communities and countries such as South Africa, where data protection laws are strongly enforced under the Regulation of General Data Protection (GDPR) and the Protection of Personal Information Act (POPIA), Nigeria struggles with protecting information relating to individuals effectively.¹⁶ Against this background, this study examines data privacy violations in Nigeria, highlighting on enforcement challenges. It argues that strong enforcement, societal consciousness, and regulatory effectiveness is vital to ensuring digital rights are effectively secured and not just recognized in law.¹⁷

1.2 Statement of the Problem

While steps were taken to regulate data protection including the NDPA in 2023, the enforcement of the rights to data privacy is still weak. Laws alone do not guarantee compliance and in practice protection of privacy is more a theory than a reality in the absence of strong institutional mechanisms and proper regulatory supervision, and remedies for violations.¹⁸

Data privacy rights exist in Nigerian laws, but the enforcement encounters several challenges. The NDPA and its accompanying regulations provide principles for

¹⁵ Law Global Hub, *Data Privacy or Data Exploitation? Testing Nigeria's Data Protection Act, 2023* (Law Global

Hub, published online) <https://www.lawglobalhub.com/data-privacy-or-data-exploitation-testing-nigerias-data-protection-act-2023/>. last accessed 25 January 2026.

¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation);

Protection of Personal Information Act 4 of 2013 (South Africa).

¹⁷ F A Nwodo and C O Amucheazi, 'Analysis of Regulatory Strategies to Ensure the Independence of Nigeria's

Data Protection Commission' (2025) 15(1) *International Data Privacy Law*.

¹⁸ Patrick Chukwunonso Aloamaka, *A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms* (2025) 4(2) *UCC Law Journal*.



protection of data, but compliance structures are weak. This enforcement gap frustrates the effectiveness of protection and results in citizens facing violations without meaningful recourse.¹⁹

A. Inadequate Institutional Capability: Regulatory bodies such as the Commission for Nigeria Data Protection (NDPC) face challenges including overlapping responsibilities, insufficient funding, and limited technical know-how.²⁰ These issues make it difficult for them to monitor compliance, investigate violations, and impose penalties.²¹ Public trust in enforcement is weakened by political meddling and corruption, which undermine the independence of the regulators.²²

B. Inefficiency in the Judiciary: The judiciary also struggles with limited technical expertise and inefficient procedures, and this hurts enforcement too. Because few judges have handled privacy cases before, rulings might come out differently, while delays and weak remedies become routine. Court processes appear to be costly, and the processes involved are complex; as a result, citizens are discouraged from seeking redress for the breach, therefore making enforcement weak.²³

¹⁹ T Ilori, 'A Postcolonial Legal Critique of the Appropriation of Online Expression in Africa' (2024) 68(1) *Journal of African Law*.

²⁰ *Nigeria Data Protection Commission – International Journal of Data Privacy and Protection* (Nigeria Data Protection Commission, 2025) <https://ndpc.gov.ng/wp-content/uploads/2025/01/NDPC-International-Journal-of-Data-Privacy-and-Protection.pdf> accessed 25 January 2026 at 8:31pm.

²¹ Data Privacy Laws in Nigeria: Compliance and Enforcement Issues (Scribd PDF, published online) <https://www.scribd.com/document/876166047/Data-Privacy-Laws-in-Nigeria-Compliance-and-Enforcement-Issues> accessed 25 January 2026 at 8:26 pm.

²² Data Protection and Privacy Laws in Nigeria: A Voyage into the NDPA General Application and Implementation Directive (GAID) 2025 (Scribd PDF, published online)

<https://www.scribd.com/document/949393814/Data-Protection-and-Privacy-Laws-in-Nigeria-a-Voyage-Into-the-NDPA-General-Application-and-Implementation-Directive-GAID-2025> accessed 25 January 2026 at 8:35 pm.

²³ *AUN Journal of Law* (2025) <https://journals.aun.edu.ng/index.php/aunijl/article/download/57/87>



C. Cultural and societal obstacles to enforcement: Cultural and social attitudes make it very hard to enforce data privacy laws in Nigeria. A lot of people prioritize being able to use digital services over knowing or protecting their legal rights. This has made privacy violations normal. This situation shows the difference between abstract and practical legal rights. Without a predictable, efficient, and responsive judicial mechanism, the enforcement of data protection laws remains a theoretical ideal rather than a practical reality.²⁴

D. Technological and Cross-Border Challenges: Enforcement is also limited by a lack of technological infrastructure and problems that arise when crossing borders.²⁵ Nigeria does not have the best cybersecurity tools or investigative resources, which makes it harder for regulators to find and fix problems.²⁶ Also, many multinational companies store or process a lot of personal data outside of Nigeria, which makes things more complicated from a legal and jurisdictional point of view.²⁷

E. Legal Incoherence and Economic Incentives: Violations happen due to uncertainty of the legal system, ambiguous rules set in place, and lack of efficient sanctions. It is hard to know what to do when regulatory bodies like NDPC, NITDA, NCC, and CBN have overlapping mandates. Companies that make money from personal data do not suffer many consequences because of weak enforcement and political reasons, which place

[accessed 25](#)

January 2026 at 8:40pm.

²⁴ J O Effoduh, "Toward A Truth Worthy and Inclusive Data Governance Policy for The Use of Artificial Intelligence in Africa" (2024) 6 *Data and policy* 34.

²⁵ Patrick Chukwunonso Aloamaka, 'Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions' (2023) 3(1) *UCC Law Journal* 281–321.

²⁶ Ibrahim Shehu and Sani Rabi Bello, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria' (2022) *Journal of Law, Policy and Globalization*.

²⁷ V C Onuchukwu, 'Big Tech, Big Risk: Regulating International Tech Giants under Nigeria's Cyber and Data Protection Laws' (2025) 7(2) *Chukwuemeka Odumegwu Ojukwu University Journal of Private and Public Law*.



people at risk of systemic privacy violations. These problems affect digital platforms, slow down Nigeria's digital economy, and show how important it is to come up with effective ways to make data privacy laws function properly.²⁸

1.3 Research Question

- i. To what extent does the existing law in Nigeria provide effective protection against the violation of data privacy in the virtual world, and to what extent does it align with international best practices like the GDPR and POPIA?
- ii. Which are the key challenges that pose difficulties in the enforcement of Nigeria's privacy legislation, amid technological advancement?
- iii. What are the prospects for the development and implementation of the legislation in Nigeria?

1.4 Aim and Objectives of the Research

The project aims to analyse the challenges in enforcing data protection laws in the contemporary digital society. The specific objectives are:

1. To evaluate the adequacy of the existing regulatory regime in Nigeria, namely the NDPA and related regulations, in addressing data privacy crimes and adherence to such international norms as the GDPR and POPIA.
2. To review the various institutional, judicial, technological, and governance obstacles to facilitating proper enforcement of data protection laws properly enforced in Nigeria, especially considering emerging technologies.
3. To review possibilities for developing and implementing data privacy laws in the country's cyberspace.

²⁸ A I Uwadinma, 'The Digital Economy and Consumer Protection in Nigeria: A Legal Analysis of Data Privacy

Laws under the Nigeria Data Protection Act 2023' (2025) 1 *AUN Journal of Law* 1.

1.5 Research Methodology

The research adopts a doctrinal approach as it focuses on the examination of statutes, regulations, judicial pronouncements, and administrative structures for data privacy in Nigeria. The central focus of the study is an examination of the NDPA 2023, related statutes, and case laws in assessing the adequacy of the enforcement model in place.

Furthermore, secondary sources like textbooks, journal articles, reports and policy documents are utilized for the research. These resources will offer valuable information on developing, interpreting and enforcing privacy laws. It uses a doctrinal research method that entails analysis of the rules, principles, and authorities from the law to uncover gaps or issues with current law.

It is qualitative as it does not depend on numbers, but rather interpretation and analysis of the law. The inquiry aims at exploring the underlying causes of poor enforcement of Nigeria's law in a broader institutional, social and technological context, and identifies desirable doctrinal and policy changes that will strengthen the protection of data privacy.

1.6 Scope of The Study

The focus of this study is largely to explore the Nigerian legal framework on data privacy and specifically its challenges in the digital era. It is based on the Nigeria Data Protection Act 2023, subsidiary regulations, regulatory instruments and court decisions. The study aims to give detailed picture of Nigeria's enforcement landscape by analysing the legal instruments. While the study is nationally focused, it recognizes that issues existing in the digital world are transnational in nature. So it benchmarks the international practices like those of the European Union and its General Data Protection

Regulation and that of South Africa and its Protection of Personal Information Act. The examples are not intended to be comprehensive, but are deliberately selected to underline the weakness in the enforcement regime and to provide transferable lessons for improvement. The research is not a technical or engineering analysis of data security nor is it empirical research using field methods such as surveys or interviews. Instead, the emphasis is doctrinal and legal, examining the problems of enforcement from the perspective of statutory interpretation, institutional performance and judicial practice.

1.7 Significance of the Study

This study is crucial as it tackles one of today's most urgent socio-technical issues – the effective implementation of data privacy in the context of fast digitalization. With the growing value of personal data as well as its potential for misuse and misuse, understanding, implementation and enhancement of data privacy standards are crucial.

Firstly, the study adds to the academic debate by analyzing the existing data security measures, identifying gaps in the enforcement system, and highlighting issues with data privacy in today's technologically advanced society. It will enrich the scholarly debate on current literature on Digital Rights, Digital Governance, and Cyber Law.

Secondly, it also provides policy relevance. It highlights the challenges and offers valuable guidance to policymakers, stakeholders, and regulators such as the Nigeria Data Protection Commission (NDPC) to enhance compliance frameworks and enforcement measures. The recommendations included in the study for filling gaps in the data privacy framework will also be beneficial to legislators and policymakers.



Last but not least, this study fills a gap in the literature on the challenges and possibilities for data privacy enforcement in Nigeria, where there is limited literature, particularly on data privacy post-2023 reform. The immediate beneficiaries of the study are digital rights activists, corporate organizations, personal data holders in the digital ecosystem, digital industry practitioners, legal scholars, judges, the NDPC, and Nigerian citizens, among whom are those who have suffered the loss of their personal data.

1.8 Literature Review

Concerns of data privacy has gained importance as individuals, businesses, and public institutions rely more heavily on digital platforms for communication, trade, and governance.²⁹ This shift to a data-driven society has placed citizens at greater risk of their personal data being collected, exploited, or disclosed without consent.³⁰ In response, Nigeria has introduced regulatory frameworks to protect personal data. However, while these laws are important, enforcing privacy rights in practice remains a major challenge.³¹

Human choices have been greatly disrupted with the expansion of modern electronic technologies, and academic discussions on privacy have changed over time. Historically, literature treated privacy as a philosophical or moral concept based on the individual's right to be left alone.³² In recent times, however, privacy is central to data protection law, reflecting the way corporations commodify personal data and governments expand

²⁹ O A Olatunbosun, 'Digital Governance and Regulatory Challenges in Nigeria' (2021) 15 *Nigerian Journal of Public Law* 87.

³⁰ U M Sadiq, 'Personal Data Protection and Privacy in Nigeria's Emerging Digital Economy' (2020) 4 *African Journal of Law and Technology* 112.

³¹ A O Arowolo, 'Enforcing Data Protection Rights in Nigeria: Legal and Institutional Constraints' (2022) 9 *Journal of African Law and Policy* 64.

³² S D Warren and L D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard law review* 193.

surveillance. This has made privacy a pressing legal and policy issue.³³ The General Data Protection Regulation (GDPR) is considered a benchmark for reconciling new technologies with rights protection.³⁴

The disparity in global implementation of data protection frameworks is highlighted through comparative research. Numerous developing countries experience a distinct disconnect between statutory provisions and real-world enforcement, while advanced economies typically benefit from strong institutions and greater public awareness, while many developing countries experience weak alignment of law and real-world enforcement.³⁵ African states can, through the Protection of Personal Information Act (POPIA), tailor global models to fit regional context.³⁶ This body of work underscores that the enforcement problems faced in Nigeria are part of a wider challenge faced by many African countries.

A big issue with the current research on data protection in Nigeria is that it tends to focus so much on what the law says on paper rather than how they work in the real world.³⁷ This gap stands out clearly in the context that Akinboade and Salami examined, who moved past the legal text to tackle the institutional hurdles that make enforcement the 'Achilles' Heels' of data protection in emerging economies.³⁸ They point out that even though the introduction of the NDPA 2023 gave Nigeria a solid formal law for

³³ D J Solove, *Understanding Privacy* (Harvard University Press 2008).

³⁴ Regulation (EU) 2016/679 (General Data Protection Regulation).

³⁵ J Colin Bennett and C D Raab, *The Governance of Privacy* (MIT Press 2006).

³⁶ J Roos, "South Africa's Protection of Personal Information Act: Lessons for Africa" (2020) 37 *South African Yearbook of International Law* 55.

³⁷ T Akinboade and D Salami, *Data Privacy and Enforcement in Nigeria: A Regulatory Perspective* (2022) 9(1)

African Journal of Law & Technology 21

³⁸ S Makulilo, 'Privacy and Data Protection in Africa: A Comparative Overview' (2016) 2 *African Journal of Information & Communication* 1.



privacy, real-world enforcement is still weak. They blamed the overlapping responsibilities and limited regulatory capacity between agencies like the NDPC, NCC, and FCCPC. Their insight to the regulatory struggle is valuable, but they did not back it up with case studies or judicial examples or offer any solutions.

This discussion builds on the earlier work of Okoye, whose legal work on the NDPR issued in 2019 by the National Information Technology Development Agency suffers similar practical in-depth because there are no actual judicial decisions or real-life examples.³⁹ He sees the NDPR as a notable achievement that brought Nigeria in line with global standards like the GDPR, introducing explicit rights for data subjects. He notes that before 2019, privacy rules in Nigeria were split across different sectors, like CBN and the NCC, with separate guidelines.⁴⁰ While he convincingly argues that the NDPR was the first step toward comprehensive reform, his article focuses mainly on explaining the law and pays little attention to how privacy rights are enforced in practice or how institutional weaknesses affect compliance.

One weakness is the current cross-border analysis; Ojo focuses on how global technology companies are meant to apply Nigerian data protection laws to companies like Google and Meta that process local data overseas.⁴¹ By comparing the extraterritorial stipulations of the NDPA with the GDPR, Ojo makes a solid case that the domestic rules are not tightened enough. His discussion reflects the global nature of

³⁹ I Okoye, 'Data Protection in Nigeria: An Analysis of the NDPR' (2021) 15(2) *Nigerian Law Journal* 45.

⁴⁰ A Adeyemi, 'Sectoral Regulation of Data in Nigeria Before the NDPR' (2018) 8 *Nigerian Journal of Technology Law* 33.

⁴¹ A Ojo, 'Cross-Border Data Transfer and Jurisdictional Enforcement: A Nigerian Perspective' (2023) 2(4) *Journal of African Cyber Law* 57

privacy violations and the limitations of purely domestic regulation.⁴² However, his solutions remain mostly theoretical. Furthermore, because his analysis predates NDPC's recent attempts towards aggressive enforcement against multinational companies, it remains unanswered whether current regulatory actions represent real progress or symbolic gestures.

Through an institutional lens, the NDPC in its 2024 Annual Report outlines the Commission's core responsibilities,⁴³ noting that over 1,000 organizations underwent audits in 2023, resulting in sanctions for non-compliance. It highlights the initiative aimed at public awareness and training data protection officers. Yet, while the report shows active regulatory presence, it lacks detailed metrics regarding overall complaints received, investigative procedures, or the long-term efficacy of its enforcement actions. This aligns with scholarly criticism that official institutional reports frequently prioritize showcasing progress over addressing the systematic challenges.⁴⁴ Without meaningful awareness and advocacy, citizens remain unable to demand accountability, leaving enforcement weak.

Finally, Oduwale offers a socio-legal perspective that explores the disconnect between the country's privacy laws and citizens' lived reality.⁴⁵ He points out that vast numbers of Nigerians are unaware of their data rights, rarely informed when their sensitive information is used and disclosed. The violations are frequently unreported partly due to cultural attitudes and low digital literacy. This reflects a wider theme in African

⁴² C kuner, *Transborder Data Flows and Data Privacy Law* (Oxford press 2013).

⁴³ Nigeria Data Protection Commission, *Annual Data Protection Report* (NDPC, Abuja 2024).

⁴⁴ E Agaba, 'Public Awareness and Data Protection in Nigeria' (2021) 19 *Nigerian Law & Policy Review* 74.

⁴⁵ K Oduwale, *Data Privacy in Nigeria: Between Legislation and Reality* (2020) 5(1) *Journal of African Legal*

Studies 33.



scholarship that even the best legal frameworks cannot succeed if the public is disengaged. As Oduwole suggests, enforcement depends not only on sanctions but also on education, advocacy, and building a culture of privacy. However, his arguments would be stronger with empirical evidence, such as surveys or case studies showing how Nigerians understand and respond to privacy violations.

The reviewed literature collectively shows that Nigeria achieved important progress in the development of a regulatory system for data protection through the NDPR and NDPA. Yet, enforcement remains undermined by institutional weaknesses, judicial inefficiencies, low public awareness, and the challenge of regulating multinational companies. Comparative studies confirm that these challenges are not unique to Nigeria but are common across Africa, where weak institutions and cultural differences complicate the adoption of global norms.⁴⁶ Earlier sector-specific regulations show how fragmented Nigeria's legal landscape once was, and while the NDPR and NDPA represent a major improvement, enforcement continues to lag behind legislation. Regulatory agencies lack adequate resources, and the judiciary is ill-equipped to handle complex technological disputes. Public awareness remains minimal, and regional cooperation, though frequently suggested, has yet to take concrete form.⁴⁷

In conclusion, the literature makes clear that while Nigeria has enacted strong privacy laws, enforcement is still the weakest link.⁴⁸ Institutions lack the capacity to regulate

⁴⁶ African Union Commission, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)* (AU 2014).

⁴⁷ United Nations Economic Commission for Africa, *Digital Transformation Strategy for Africa (2020–2030)* (UNECA 2020)

⁴⁸ L Adebayo, *Data Protection and Enforcement in Nigeria: Regulatory Capacity and Challenges* (Springer 2023) 45–67.



effectively,⁴⁹ the courts face challenges in handling privacy disputes, and the public is largely unaware of its rights. The global model of the GDPR has influenced Nigerian law,⁵⁰ but socio-economic and institutional realities limit its practical impact. Future research should move beyond describing the existence of laws to examining enforcement practices, identifying institutional barriers, and suggesting workable reforms. Only then can Nigeria translate legislative progress into real protection for its citizens in the digital age.⁵¹

⁴⁹ Ibid 50–52.

⁵⁰ S Eze, 'The Influence of the GDPR on Emerging Data Protection Frameworks: The Nigerian Experience' (2023)

8 *International Data Privacy Law* 221, 226.

⁵¹ S Eze, 'The Influence of the GDPR on Emerging Data Protection Frameworks: The Nigerian Experience' (2023)

8 *International Data Privacy Law* 221, 230.



CHAPTER TWO

CONCEPTUAL AND THEORETICAL FRAMEWORK

2.1 Conceptual Framework

2.1.1 Defining data

Data privacy is essential since data is the foundation of information.⁵² The variation in definitions among different regulations underscores the necessity of comprehending how personal information is gathered, utilized, and preserved.⁵³ The importance is seen when discussing people's rights in the digital environment.⁵⁴

Data is described as raw variables, metrics, or symbolic inputs collected for retention and analytical synthesis to guide decision-making. These representations can be numerical, textual, biometric, visual, or sensor-generated.⁵⁵ According to the Oxford Learner's Dictionary, data essentially means two things: raw information collected to help people make decisions, and information managed by a computer.⁵⁶

Under NDPR 2019, data is legally recognized as the foundational symbols, characters, and binary units processed by computing systems. This includes any information transmitted through digital signals or preserved across different storage media.⁵⁷ This definition reflects the technical nature of data in digital systems. The NDPR also

⁵² A Solove, *Understanding Privacy* (Harvard University Press 2021) 15.

⁵³ R Clarke, 'Definitions of Data in Information Governance' (2019) 14 *Journal of Information Privacy and Security* 33, 35.

⁵⁴ L Floridi, *The Ethics of Information* (Oxford University Press 2013) 22–23.

⁵⁵ R Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (Sage 2014).

⁵⁶ Oxford Learner's Dictionary (Oxford University Press, 2023) 'Data'

<https://www.oxfordlearnersdictionaries.com>

accessed 27 January 2026 at 2:40 am.

⁵⁷ Nigeria Data Protection Regulation 2019, part 1



identifies the key actors in data processing. Section 65 categorizes these entities into controller, processor, and subjects as: Data controller is any person, private enterprise, public authority, or institution that independently or collaboratively determines the purposes and methods of processing personal information; Data processor denotes any independent party, corporate firm, state body, or external entity who handles personal information based on the instructions of a controller or authorized processor; Data subject represents the specific individual the information describes.”⁵⁸

Personal data encompasses any details associated with a specific, recognizable individual known as a data subject. It includes any marker like location information, online identifiers, that can pinpoint a person’s identity either on its own or when combined with other clues. The General Data Protection Regulation (GDPR) Article 4 functions as the definitive benchmark for modern privacy frameworks. It interprets personal data as any details regarding an individual that can be recognized from that data alone or by cross-referencing it with external details.⁵⁹

The Nigeria Data Protection Regulation 2019, in part one, defined personal data to include “information relating to an identified or identifiable natural person, including identifiers such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. It could include a name, address, photo, email address, bank details, social media posts, and other unique identifiers such as Media Access Control address (MAC), Internet Protocol address (IP), International Mobile Subscriber Equipment number (IMEI), International Mobile Subscriber Identity number

⁵⁸ Nigeria Data Protection Act 2022, section 65

⁵⁹ European Union, General Data Protection Regulation (EU) 2016/679 [2016] OJ L119/1



(IMSI), Subscriber Identity Module (SIM), or other personally identifiable information (PII).”⁶⁰

Building upon the NDPR 2019, the NDPA 2023 introduced a robust statutory structure for safeguarding individual information. Section 65 of the Act defines personally identifiable information as any data that distinguishes a specific human being, either directly or through unique personal characteristics. It includes classifications like name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, psychological, cultural, or socio-economic identity.⁶¹

The NDPA improves upon the NDPR by providing a clearer definition and creating the Nigeria Data Protection Commission (NDPC). It is an independent regulatory entity tasked with supervisory control, maximizing transparency, and elevating user privacy standard while maintaining the fundamental components of the NDPR 2019.

Grasping the definition of data remains fundamental to this discussion, as safeguarding individual privacy forms the foundation of current online governance and privacy regulations.⁶² Massive amounts of private information are gathered, processed, transmitted, and archived by state institutions and commercial organizations as societies become more dependent on digital technologies. This raises important issues regarding regulation, accountability, and individual rights. The type, scale, and vulnerability of the collected information determine the strictness of legal protection required, as well as specific duties placed on controllers and processors. It establishes the foundation for understanding user privacy rights, corporate responsibilities, and the broader consequences of statutory compliance or failure by precisely defining data and

⁶⁰ Nigeria Data Protection Regulation 2019.

⁶¹ Nigeria Data Protection Act 2023

⁶² Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press 2020).

personal data.

2.1.2 Defining Data Privacy

Analyzing data privacy principles is essential in understanding the regulation of personal information within the digital landscape. At its core, this concept centers on individuals' autonomy regarding the way their private details are gathered, handled, archived, or disseminated. It operates on the fundamental premise that personal records about an individual ought not be accessed or used without their prior knowledge and consent. The Supreme Court's decision reinforced the principle of consent in *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo*⁶³, where the Court recognized the right of individuals to make decisions affecting their private lives and personal autonomy. The reasoning in the case aligns closely with modern data protection principles requiring informed consent before personal information is processed. In contemporary digital society where private citizen data is perpetually generated, transmitted and saved, the importance of protecting privacy has become increasingly significant.

Historically, the concept was framed in physical terms as the basic freedom from unwanted intrusion. However, modern legal academic discourse has expanded this meaning to include informational privacy. In this view Alan conceptualizes privacy as the capacity of individuals to independently decide the timing, manner, scope of sharing their personal details.⁶⁴ The shift reflects the movement from physical privacy to data-

⁶³ (2001) 7 NWLR (Pt 711) 206

⁶⁴ A F Westin, *Privacy and Freedom* (Atheneum 1967) 7.

driven privacy concerns.

While privacy as a general concept is not a new idea, the growing dependence on data-driven technologies has led to the creation of a unique area in the law, and conceptually, the protection of data privacy.⁶⁵ Ogban-Iyam asserts that privacy is viewed as a component of individual freedom, especially given the increasingly digital environment interaction and record-keeping.⁶⁶ Similarly, Oyewole on the notion that Nigerians' right to privacy entails safeguarding against both government overreach and the increasing prevalence of private digital platforms that gather copious amounts of personal data.⁶⁷ Nwankwo views data privacy as the foundation that protects human freedom in an age where government agencies, businesses, and applications continue to collect and analyze personal information.⁶⁸

Data privacy encompasses a vast spectrum of data types, encompassing names and addresses, biometric identifiers, digital behavior, financial data, and geolocation information.⁶⁹ It suggests a balance between individual rights and societies or commercial interests. While individuals have an interest in the control over their data, governments and corporations may then need access to information for purposes like security, service provision or economic activity.

⁶⁵ A O Ayeni. 'The role of the African Commission in enhancing implementation monitoring through dialogue and documentation' (2024) 24(2) *African Human Rights Law Journal* 937–961.

⁶⁶ J A Ogban-Iyam, "Privacy and the Dynamics of Social Control in Modern Nigeria," *Nigerian Journal of Social Sciences* (2014).

⁶⁷ O Oyewole, "Re-thinking Privacy Rights in Nigeria's Digital Environment," *Nigerian Journal of Public Law* (2019).

⁶⁸ C Nwankwo, "Digital Rights and Data Protection in Nigeria," *Journal of African Law and Technology* (2020).

⁶⁹ T Ilori, 'Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Revised Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2024) 24(1) *African Human Rights Law Journal* 1–30.

This concept thus involves an understanding of competing values such as autonomy vs. efficiency, liberty vs. security, and control vs. innovation; Nissenbaum views the understanding of privacy must be weighed against the competing social, economic, and technological interests. According to her, privacy is relative and has to be balanced against other ideals such as security, efficiency, and innovation. She believes privacy should be protected in ways that respect the social context within which people share information.

In legal terms, it is both a rights-based and regulatory concept. From a rights perspective, it serves to protect personal sovereignty, individual liberty, and freedom from unreasonable interference.⁷⁰ As a regulatory framework, it places obligations on data-handling entities to behave responsibly, transparently and accountably. This dual nature shows that the concept of data privacy operates at the intersection of individual rights and collective regulation.

The idea also involves the notion of proportionality. The information to be collected and processed should only be what is necessary and relevant and not excessive or arbitrary. Proportionality guarantees that the privacy rights are not infringed by indiscriminate or blanket surveillance.⁷¹ In this sense, data privacy is one of those principles that informs the limitation of power, as well as the ethical use of information in general.

Data privacy should also not be confused with data security, but the relationship between the two is tight. Security is concerned with preventing data from being

⁷⁰ B Faturoti and I Juma, "Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice," *International Review of Law, Computers & Technology* (2025): 1–25.

⁷¹ O Babalola, "Transborder Flow of Personal Data (TDF) in Africa," *Computer Law & Security Review* 52 (2024).

accessed or compromised in some way, whereas privacy is concerned with ensuring that data is used appropriately and legally. Both are important in terms of the protection they provide, but privacy is wider in definition, covering ethical, legal, and social aspects beyond technical security.⁷²

In conclusion, data privacy is a multi-layered concept that encompasses individual rights, regulatory compliance, ethical considerations, and societal trust. It is a dynamic concept that changes with technology and describes the balance between individual interests and common interests. Thus, a holistic interpretation of data privacy is vital when approaching the issues of enforcement in the digital environment in Nigeria.⁷³

2.1.3 Context of the Digital Age: Technology, Data and Society

In the Nigerian setting, the modern technological era represents a restructuring of daily existence, work, and interaction, with digital technologies and platforms increasingly embedded within the fabric of society. Several government agencies and private institutions now depend on big data systems for service delivery. These developments suggest that, rather than simply technology, it is the way in which digital systems and data mediate social, economic, and institutional life that characterizes the digital era, both globally and in Nigeria. From cellphones to cloud computing, technology has now assumed a central place in daily life, influencing not only social interactions, but also business, governance, and communication. Like some businesses and marketers have also embraced data-driven means through which to target and engage customers,

⁷² B Fatureti and I Juma, "Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice," *International Review of Law, Computers & Technology* (2025): 1–25.

⁷³ T Ilori, 'Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2023) 23(2) *African Human Rights Law Journal*.



revealing how digital technologies shape commerce and social intercourse.⁷⁴ On another score, the rapid shift from paper records to digital platforms has created new challenges to confidentiality and privacy in Nigerian universities and institutions while gaining efficiency.⁷⁵

The near-ubiquitous use of digital platforms has altered how information is produced and consumed, turning personal data into both a by-product of everyday living and a commodity in itself.⁷⁶ Data growth is one of the hallmarks of the digital age. Every time we complete an online transaction, communicate over social media, or use a mobile app, data points are created that can be stored, analyzed, and re-used. Unlike earlier times, data are now collected passively and constantly, often without conscious knowledge of a person's actions. The invisible buildup of this information poses deep questions about autonomy and consent. Technology has also changed the size and speed of data processing.⁷⁷ Driven by advancements in predictive modeling, pattern recognition, and advanced computational algorithms, organizations possess the capability to evaluate massive datasets in real-time to forecast behavior, personalize services, and drive efficiency. While these innovations provide operational optimization and economic benefit, they simultaneously amplify the dangers linked with surveillance and manipulation, as individuals become increasingly "seen" by institutions. In the digital era, personal information is no longer restricted to information voluntarily

⁷⁴ R O Mohammed, A Musa and Z O Ismail, 'Big Data Adoption and E-Government Implementation in Nigeria' (2022) 12 *ATBU Journal of Science, Technology & Environmental Education*.

⁷⁵ S N Ugbo, K Ajilore and O Ajaegbu, 'Big Data Analytics Adoption in Brand Communication Campaigns: Evidence from Lagos State, Nigeria' (2021) *International Journal of Cambridge Research Publication*.

⁷⁶ O Babalola, "Transborder Flow of Personal Data (TDF) in Africa," *Computer Law & Security Review* 52 (2024).

⁷⁷ A Omotubora, "Privacy by Design and the eNaira: Ensuring Data Protection in Nigeria's Central Bank Digital Currency," *Journal of African Law* 68, no. 2 (2024).

provided by an individual. Easy-to-understand and descriptive, metadata is being continuously created by application devices and platforms, including location traces, usage patterns, and interaction histories. While this metadata may seem harmless, when it's aggregated and analyzed, it can be used to identify extremely personal things about the individual. The consequences for privacy are significant, as there's less control over information about yourself.

Also, the rapport between data and society has changed. Nowadays, people very willingly share personal information to get a service, many times without realizing the broader implications of such an action. This "trade-off" society normalizes data surveillance and commodification. As scholars have described it, "digital dependency" involves situations in which privacy is considered less valuable than the convenience of use. Additionally, the use of the digital sphere has extended the reach of governments.⁷⁸

Government agencies are dependent on digital surveillance for crime prevention and intelligence gathering, and public institutions depend on data to deliver services.⁷⁹ While in some contexts these practices are defensible, they set up tensions between public interest and constitutional liberties.⁸⁰ In the digital age, therefore, tensions over the limits of permissible intrusion are renewed. Digital platforms make things more complicated.⁸¹ Data moves easily across borders, while national laws cannot regulate or

⁷⁸ L Ozeran, A Solomonides and R Schreiber, 'Privacy versus Convenience: A Historical Perspective, Analysis of

Risks, and an Informatics Call to Action' (2021) 12 *Applied Clinical Informatics* 274.

⁷⁹ T Ilori, 'A postcolonial legal critique of the appropriation of online expression in Africa', *Journal of African Law*, 2024, pp 68(1).

⁸⁰ Charles Fried, 'Privacy' (1970) 77 *Yale Law Journal* 475, 477–79.

⁸¹ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010) 53–56.



control it.⁸² A user in Nigeria may engage with a platform based in another jurisdiction, which highlights the uncertainties regarding how far state-level privacy statutes apply beyond local borders.⁸³ As with so many other environmental issues, enforcement is not only a national problem, but increasingly an international one. This digital divide adds to the problem in Nigeria.⁸⁴ While digital literacy and awareness of the risks of privacy breaches are likely higher in urban populations, many rural communities use technology without fully understanding what it entails.⁸⁵ This unbalanced consciousness confirms vulnerabilities and weakens enforcement as public demand for accountability is too weak.⁸⁶

In conclusion, the digital era is one of both opportunity and risk. On one side, it is improving communication, innovation and social interaction. On the other it puts individuals at risk of a level of intrusion into their private lives they have never faced before. Understanding this duality is crucial for contextually situating data privacy breaches and for framing interventions to counter them.⁸⁷

2.1.4 Type of Data Privacy Breaches

⁸² G W Greenleaf, 'International and Regional Commitments in African Data Privacy Laws' (2022) 46 *Computer*

Law and Security Review 105743.

⁸³ O Babalola, 'Transborder Flow of Personal Data (TDF) in Africa' (2024) *Computer Law & Security Review* 52.

⁸⁴ T Ilori, 'Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Revised Declaration of

Principles on Freedom of Expression and Access to Information in Africa' (2024) 24(1) *African Human Rights Law Journal* 1–30.

⁸⁵ S N Ugbo, K. Ajilore and O. Ajaegbu, 'Big Data Analytics Adoption in Brand Communication Campaigns: Evidence from Lagos State, Nigeria' (2021) *International Journal of Cambridge Research Publication*.

⁸⁶ A A Anyaegbunam, 'Legal and Institutional Framework for Data Protection in Nigeria' (2020) *Nnamdi Azikiwe*

University Journal of International Law and Jurisprudence 87

⁸⁷ J O Effoduh, 'Toward a Trustworthy and Inclusive Data Governance Policy for the Use of Artificial Intelligence in

Africa' (2024) 6 *Data and Policy* 34.



Data privacy breaches are defined as any handling of personal information that violates defined legal, ethical, or social standards. Such breaches affect the individual's entitlement to regulate their own private data, while the consequences are often material, such as loss of money, damage to reputation, or psychological harm.⁸⁸ The forms of these violations vary, depending on the multi-faceted channels through which data is generated and utilized within contemporary society. The most common form of violation is unauthorized access, sometimes called a data breach.⁸⁹ These happen when personal information is disclosed without permission by hackers, insiders, or careless individuals.⁹⁰ Sensitive information or identification details can be compromised, leading to potentially devastating consequences, such as identity theft and fraud. Another type of offense stems from the misuse of consent. Agreement from the user serves as lawful justification for a vast amount of information handling on digital platforms, but often such consent is uninformed, forced, or buried in long terms and conditions.⁹¹ This undermines the consent mechanism and makes it possible for entities to exploit private records in the name of the law.⁹²

Data Privacy breaches also happen as a result of information being collected when it is unnecessary or excessive. For example, platforms can sometimes require more information than is reasonably necessary for a service. This violates the concept of data

⁸⁸ B Atoyebi and A Omotubora, 'Data Protection Regulation and Enforcement in Nigeria' (2020) 4 Nigerian Journal of Technology Law 55.

⁸⁹ C J Bennett and C D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006)

⁹⁰ A Edgcumbe, J Currie and S McLennan, 'Potato Potato? Disentangling De-identification, Anonymization, and Pseudonymization in Data Protection Law' (2025) 12(1) Journal of Law and the Biosciences Isae029.

⁹¹ G Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press 2014)

⁹² J E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 35–40.



minimization, thereby placing people at higher risk where the data is misused or compromised. Profiling and algorithmic manipulation are a less obvious type of violation.⁹³ By leveraging the power of personal data, companies can build in-depth profiles of individuals, anticipate behavior, and drive decisions. While such practices have the potential to improve user experience, they also raise issues regarding autonomy, fairness, and discrimination. The inability of algorithms to be transparent increases these risks.⁹⁴

Cross-border data transfers add a third layer to the violation.⁹⁵ Additionally, if personal data is exported from Nigeria for processing outside the country, the protection of the data under domestic law may be lost at that time. This raises questions of sovereignty, responsibility and adequacy of foreign legal regimes. In such cases, individuals are very vulnerable since there are no strong mechanisms for international cooperation.⁹⁶

State surveillance can also be a violation where it goes beyond the lawful limits.⁹⁷ While a government may have a national security justification for surveillance, indiscriminate or excessive monitoring destroys the essence of data privacy. Getting the balance right between the security imperatives and individual rights protection is difficult.⁹⁸ Data Privacy breach, a breach of privacy goes beyond direct harm to individuals.⁹⁹ At a

⁹³ De Hert and V Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the

Protection of Individuals?' (2016) 32 Computer Law and Security Review 179.

⁹⁴ J E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 35–40.

⁹⁵ A F Westin, *Privacy and Freedom* (Atheneum 1967).

⁹⁶ C Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 7–10

⁹⁷ B O Nwabueze, *Constitutional Democracy in Africa* (Spectrum Books 2003).

⁹⁸ David Lyon, *Surveillance Studies: An Overview* (Polity 2007) 89–92.

⁹⁹ G W Greenleaf, 'International and Regional Commitments in African Data Privacy Laws' (2022) 46 *Computer Law and Security Review* 105743.



societal level, rampant violations undermine public trust in digital platforms, and discourage participation in the digital economy. This breakdown of trust erodes the revolutionary power of technology and reinforces inequality because people disengage from services because they are afraid of abuse. Further, the nature of violations depends on the level of technological sophistication. As cyber criminals are evolving in more sophisticated ways, such as phishing, ransomware or deepfake technologies, enforcement agencies are struggling to match their sophistication. This technology arms race gives rise to an ever-present enforcement gap where the vulnerable are left exposed despite the existence of a legal protection.

In conclusion, violations of data privacy are complex and they include illegal access, breach of consent, over-collection, profiling, cross-border transfers and state surveillance. Their reach is individual and social, local and global. It is important to know the extent and complexity of these violations to analyze the reasons why enforcement is difficult in Nigeria and to suggest effective reform measures to tackle its issues.¹⁰⁰

2.1.5 Defining Enforcement, Challenges, and Prospects

2.1.5.1 Enforcement

Enforcement is ensuring that people, companies, or public bodies comply with established information security standards. It is what transforms written laws into real protection for people's private data. Privacy laws may exist, but have minimal impact if they are not enforced. According to Solove and Schwartz, "Enforcement is what bridges the gap between formal legal rights and real-world protection by adding elements such

¹⁰⁰ T Ilori, 'Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2023) 23(2) *African Human Rights Law Journal* 899–923.



as monitoring, accountability, and remedies.”¹⁰¹

In Nigeria, enforcement of data privacy is executed through the provisions of the NDPR 2019 and the NDPA 2023. According to Uwadinma, such legislation ensures that an organization remains accountable for any personal records under their care.¹⁰² Supervision over these data practices falls under the purview of the NDPC. Okpara and Okpara suggest that individuals should equally have strong procedures for complaint, redress, or legal contestation to counter the unlawful handling of their private records by processing parties. Without these opportunities, the enforcement cannot be complete since the rights exist yet cannot be so well defended.¹⁰³

Globally, enforcement is more complicated because data often crosses borders. Schwartz and Korte add that this calls for international cooperation and harmonization of rules for enforcement to be effective.¹⁰⁴ The enforcement of privacy concerns should also strike a balance with protection, innovation, economic growth, and freedom of expression, to which Nigeria, with its growing digital economy, is very relevant.¹⁰⁵ Enforcement is, thus, central because it represents the major avenue through which privacy laws are made real and meaningful.

¹⁰¹ D J Solove and P M Schwartz, *Information Privacy Law* (5th edition, Aspen Publishers 2021).

¹⁰² A I Uwadinma, 'The Digital Economy and Consumer Protection in Nigeria: A Legal Analysis of Data Privacy

Laws under the Nigeria Data Protection Act 2023' (2025) 1 AUN Journal of Law.

¹⁰³ C Okpara and A Okpara, 'Data Protection, Individual Remedies and Enforcement Challenges in Nigeria' (2021)

Nigerian Journal of Law and Practice.

¹⁰⁴ P M Schwartz and Gert-Jan Korte, 'Transnational Data Flows and Enforcement Challenges' (2019) 37 Computer

Law and Security Review 105.

¹⁰⁵ A E Akintayo, 'Trends and Implications of Nigerian Courts' Jurisprudence on Privacy and Data Protection:

Lessons from Comparative Foreign Jurisprudence' (2024) 1 African Journal on Privacy & Data Protection 99–

118.



2.1.5.2 Challenges

Challenges are conditions that make effective enforcement of the privacy laws difficult. Large amounts of personal data are collected, aggregated, and cross-referenced as digital technologies and networks proliferate, according to Aaron Olaniyi. This raises privacy risks and makes it challenging to uphold traditional ideas of control over personal data.¹⁰⁶

The challenge is compounded by the rapid digital adoption of mobile banking apps, fintech platforms, and biometric identification systems that have mushroomed in Nigeria. Aloamaka remarks that regulators need to renew their tools and skills continuously to match the emergence of new technologies, and this sometimes outstrips their institutional capacity.¹⁰⁷ Further, the limitations of staff, technical skills, and funding also pose constraints on how the NDPC can supervise and investigate possible violations. Cyber security threats, including hacking and phishing, also demand highly skilled regulatory responses.¹⁰⁸ Ukwueze underscores the problem of weak institutional capacity as a major challenge to enforcement.¹⁰⁹ This weakens trust in the system and undermines the effectiveness of the laws themselves.

Gaps in laws and policies further complicate enforcement. As Uwadinma elucidates, the advent of new technologies and cross-border data flow is usually partially unregulated

¹⁰⁶ A O Salau, 'Cybersecurity, state surveillance and the right to online privacy in Nigeria: a call for synergy of law

and policy' (2024) 1 *African Journal on Privacy & Data Protection* 152, 160–161.

¹⁰⁷ P C Aloamaka, 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms' (2025) 4 *UCC Law Journal* 242.

¹⁰⁸ P C Aloamaka, 'Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions' (2023) 3(1) *UCC Law Journal* 281.

¹⁰⁹ F Ukwueze, 'Strengthening Personal Data Protection in Nigeria' (2021) *The Nigerian Juridical Review* [unpaginated].



or not very clear; hence, there is legal uncertainty.¹¹⁰ The conflicting roles of NDPC with agencies like NITDA further complicate enforcement. Public awareness is also quite low.¹¹¹ According to Aloamaka, enforcement is best when people are aware of their rights and can report violations. Cross-border data adds more complications, including the need for international cooperation in terms of enforcement.¹¹² Moreover, cross-jurisdiction issues make it difficult for law enforcement given that global firms that deal with data from Nigeria would not be directly controlled by law enforcement in the country. Westin emphasizes that there is a need for collaboration globally to meet such challenges.

2.1.5.3 Prospects

Prospects are considered opportunities, facilitating factors, and positive developments that may improve the enforcement of data privacy. The creation of separate regulatory authorities and robust bodies of law provides a potential basis for better enforcement if these bodies have a charter, powers, and sufficient resources.¹¹³ Tools used in technology also provide opportunities for enforcement. They include automation in surveillance, encryption, and risk-compliance methods.¹¹⁴

¹¹⁰ A I Uwadinma, *Data Privacy and Consumer Protection in Nigeria's Digital Economy: A Legal Examination of the Nigeria Data Protection Act, 2023* (University of Abuja Press 2025) 45.

¹¹¹ M Eseyin and S Archibong, 'An Examination of Surveillance Capitalism and the Erosion of Data Privacy in the Digital Economy in Nigeria' (2025) *Uniuyo Law Journal* 15–17.

¹¹² J Smith and R Jones, *Cybersecurity and Data Protection: Emerging Threats* (2nd edn, Oxford University Press 2021) 112.

¹¹³ D J Greenleaf, 'Global Data Privacy Laws 2021: Current Status and Prospects' (2021) *Computer Law & Security Review* 101673.

¹¹⁴ G C Omede and F O Okorodudu, 'Cyber Security and Data Protection as Tools for the Attainment of a Smart Nation: The Nigerian Example' (2024) *International Journal of Research and Innovation in Applied Science*



In Nigeria, legislation such as NDPR and NDPA offers a basis for taking advantage of this potential by providing clarity, authority, and remedies. Institutional strengthening of NDPC, including improved funding, training are effective for enforcement. To prevent occurrences of data privacy violations from happening in the first place, proactive methods include actively monitoring of compliance, interaction with organizations, building technical capacity, enforcement based on risk, raising awareness, and cooperation with other bodies.¹¹⁵ Furthermore, awareness and technology savvy will improve regulations since people will be better placed in understanding their rights and responsibilities. At a conceptual level, prospects function as enabling factors in the framework, showing how enforcement outcomes can be improved notwithstanding existing challenges.¹¹⁶

2.2 Theoretical Framework

2.2.1 Privacy Protection Theories

2.2.1.1 Right to privacy theory

The original influential theory on the Right to Privacy advanced by Samuel Warren and Louis Brandeis in the famous Harvard Law Review Article; they stated that privacy is the "right to be let alone."¹¹⁷ This theory regarded privacy as a legal right that was independent of property or contractual rights. Its focus on protecting individuals from intrusive publicity was the basis of modern privacy law.¹¹⁸ They made this assertion

577–583.

¹¹⁵ A Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of

Ontario January 2011) Principle 1, 'Proactive not reactive; preventive not remedial'

https://en.wikipedia.org/wiki/Privacy_by_design accessed 2 February 2026 at 2:44am.

¹¹⁶ A A Anyaegbunam, 'Legal and Institutional Framework for Data Protection in Nigeria' (2020) *Nnamdi Azikiwe*

University Journal of International Law and Jurisprudence 87.

¹¹⁷ S D Warren and L D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

¹¹⁸ D J Solove, *Understanding Privacy* (Harvard University Press 2008) 23



grounded in the conviction that individuals possess an inherent ethical and legal right to determine whether and how any private activities, thoughts, emotions, or personal details may be disclosed. Warren and Brandeis understood privacy as a right protecting one's dignity, peace of mind, and psychological security from intrusive publicity insofar as the conventional doctrines of property and defamation were not equipped to deal with the type of injury occasioned by new technologies like photography and mass media, which made intimate details highly disseminable. In the Nigerian context, the theory in this regard is highlighted by the fact that privacy is an essential entitlement under constitutional and statutory law.¹¹⁹

2.2.1.2 Control theory of privacy

Another major approach revolves around the Control Theory of Privacy. Westin asserted that privacy centers on a person's capability to regulate the distribution of their personal information. He defined privacy as the right of the person to decide the timing, methodology, and scope under which details regarding the person are disclosed to others.¹²⁰ This theory is very applicable within digital environment where individuals tend to lose control of their data as a result of non-transparent collection processes and manipulative consent procedures. This regulation, in the digital age, is becoming increasingly ineffective due to misinformation in permission processes and obscurity within data collection technology. According to Westin, the essence of privacy is rooted in the power of an individual to make an informed choice about the flow of their

¹¹⁹ A Edgcumbe, J Currie and S McLennan, (2025). 'Potato potato'? Disentangling de-identification, anonymization, pseudonymization in data protection law *Journal of Law and the Biosciences*, 12(1), Isae029.

¹²⁰ A F Westin, *Privacy and Freedom* (Atheneum 1967).

information, which very often is compromised these days, for example, when apps force users to click "Accept All" to continue without clearly explaining what data would be collected or how it would be used.¹²¹ These actions highlight how modern digital systems frequently deny users the very informational sovereignty that Westin believed was at the heart of privacy.

2.2.1.3 Contextual Integrity Theory of Privacy

Helen Nissenbaum's Contextual Integrity Theory of Privacy has a lot more to do with the relevance of information flow in a certain setting than it does with secrecy. Thus, for instance, a person's medical information has to remain in a healthcare setting and cannot be used for the purpose of commercial advertisement. This argument suggests that in all cases where information moves out of a certain social setting, no matter how voluntary it was in the first instance, privacy has been violated due to a lack of relevance in accordance with certain norms of trust for which it was initially shared.¹²² Similar to this would be situations like telecommunication firms and online loan firms providing access of users' personal data to advertisers would be violative of this norm.¹²³ The federal high court held that "personal data collected for purposes of national identification will not be processed and disclosed unless a reasonable ground for doing so exists."¹²⁴ This emphasized that it is when privacy violations occur due to data being leaked out of context, as in Fried's Hypothesis, that has been further developed in

¹²¹ Fred Cate, 'The Failure of Fair Information Practice Principles in Consumer Protection in the Age of the Information Economy (Ashgate 2006).

¹²² H Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010) 42–45.

¹²³ Afeez Oyetoro, 'Data Privacy and Consumer Protection in Nigeria' (2020) Nigerian Journal of Commercial Law.

¹²⁴ Digital Rights Lawyers Initiative v National Identity Management Commission (FHC/ABJ/CS/105/2021) (FHC, 22 March 2022).

relation to Nissenbaum's Theory of Contextual Integrity.

2.2.1.4 The Panoptic Surveillance Theory

Another theory explains why digital data transfers across contexts tend to feel like violations even when individuals originally disclosed the data voluntarily. The Panoptic Surveillance Theory, which takes its name from Jeremy Bentham's Panopticon¹²⁵ (18th century) and further emerged through the work of thinkers like Michel Foucault, has defined privacy as being under threat of being overlooked.¹²⁶ He contends that people's privacy is endangered when they are constantly in danger of being watched, which causes them to internalize monitoring and change their behavior.¹²⁷ In contemporary digital systems, this surveillance is algorithmic and embedded into databases that keep track of individuals at all times.¹²⁸ This theory thus explains how the internalization of surveillance may affect the behavior of individuals in Nigeria and beyond, who may find themselves changing their behavior online even without any direct coercion. Since data from platforms is combined in ways that would never be expected by users, it becomes challenging for users to discern between public data and personal data, since it has weakened traditional privacy protection laws.¹²⁹ Companies are also able to track users even when they are no longer using the software through tracking pixels and analysis, which prompts users to be self-censoring. Financial institutions, loan apps, and telecom companies constantly monitor users, making them conscious about their online

¹²⁵ J Bentham, *The Panopticon Writings*, ed Miran Božovič (Verso 1995) (original manuscript 1791)

¹²⁶ M Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books 1975) 195–200

¹²⁷ Ibid.

¹²⁸ D Lyon, *Surveillance Studies: An Overview* (Polity Press 2007).

¹²⁹ M Burri (ed), 'Safeguarding Privacy and Other Users' Rights in the Age of Big Data' in *Big Data and Global*

Trade Law (Cambridge University Press 2021).

behaviors to avoid their data from being misused.¹³⁰

2.2.1.5 The Human Dignity Theory of Privacy

Ruth Gavison grounds privacy in the concept of human dignity, arguing that it is an essential condition for human freedom and personal flourishing.¹³¹ Privacy, on this view, encompasses not merely confidentiality but the ability to control one's sphere of social access. In the Nigerian context, this theory strengthens the argument that data privacy must be treated as a fundamental human right, not merely a matter of regulatory compliance obligation. It aligns with constitutional protections of privacy and broader human rights principles.¹³² Gaps in enforcement therefore constitute not just legal or institutional failures but also raise concerns about the violations of the human dignity and personal autonomy of Nigerian data subjects.

2.2.2 Theories of the Rule of Law and Compliance

2.2.2.1 Deterrence Theory

This is one of the basic theories of enforcement, dating back to the time of Cesare Beccaria in his book *On Crimes and Punishments*.¹³³ Deterrence Theory holds that people obey the law because the expected punishment for breaking it outweighs the expected benefit of the wrongdoing; certainty, swiftness, and proportionality of sanctions increase the likelihood of compliance.¹³⁴ In the context of data privacy, deterrence theory would suggest that regulators must impose meaningful penalties and take high-profile enforcement actions under statutes such as the Nigeria Data

¹³⁰ J E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012).

¹³¹ Ruth Gavison, 'Privacy and Limits of Law' (1980) 89(3) *Yale Law Journal* 421.

¹³² Constitution of the Federal Republic of Nigeria 1999 (as amended), section 37.

¹³³ C Beccaria, *On Crimes and Punishments* (tr Henry Paolucci, 1963) (originally published 1764).

¹³⁴ A Bottoms and A von Hirsch, 'The Crime-Preventive Impact of Penal Sanctions' in Anthony Bottoms and Andrew von Hirsch (eds), *The Oxford Handbook of Criminology* (4th edn, Oxford University Press 2012).



Protection Act 2023 to deter companies and individuals from violating privacy norms. Without adequate sanctions, violations remain a low-risk, high-reward activity for profit-seeking digital platforms.

2.2.2.2 Rational Choice Theory (RCT)

It is an extension of deterrence, which was developed by Gary Becker, and it explains conformance to the law as a rational calculation of costs and benefits.¹³⁵ Rationally, then, actors will decide to break the law if the chances of being detected and punished are low.¹³⁶ The actors in this theory include the data controllers, data processors, digital platforms, public institutions, and individual offenders. An analysis of costs vs. benefits is carried out by these actors to assess the benefits that could be gained by Illegitimate activities like profit-making potential or ease of execution, weighed against the potential costs that could be incurred.¹³⁷ This theory is very relevant in Nigeria, where due to the weak institutional capacity which includes weak detection, limited sanctions and delayed enforcement, data controllers may perceive privacy violations as economically beneficial.

2.2.2.3 The Institutional Theory of Enforcement

Douglass North demonstrated that formal rules such as laws and regulations and informal norms, habits, operating through institutions, shape the performance of legal systems.¹³⁸ Where institutions are weak, fragmented, or captured by vested interests, legal compliance becomes unpredictable. The existence of formal rules alone does not

¹³⁵ G S Becker, *The Economic Approach to Human Behavior* (1968).

¹³⁶ R V Clarke and D B Cornish, 'Modeling Offenders' Decisions: A Framework for Research and Policy' in Michael Tonry (ed), *Crime and Justice: An Annual Review of Research* (vol 6, University of Chicago Press 1985).

¹³⁷ Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76(2) *Journal of Political Economy* 169.

¹³⁸ Douglass North, *Institutions, Institutional Change and Economic Performance* (Cambridge press 1990)



guarantee compliance. In Nigeria, weak institutional coordination, overlapping regulatory mandates, and limited technical capacity reduce the effectiveness of data protection and enforcement. This theory explains why the existence of laws alone is insufficient without strong institutional structures.

2.2.2.4 The Rule of Law Theory

The rule of law theory, which was made popular by AV Dicey, emphasizes that laws must be enforced in a consistent, transparent, and equal manner.¹³⁹ The doctrine is flawed when the regulatory bodies engage in selective justice, which is punishing some parties and refusing to take action against others.¹⁴⁰ For instance, although statutory boundaries for legitimate data handling are set in place by the regulatory bodies, actual execution still remains weak, and powerful entities rarely face investigations or punitive measures.¹⁴¹ Therefore, those who break the law believe they will never be punished. This selective enforcement has led to an erosion of societal confidence in the framework that governs data privacy law enforcement.¹⁴² Grounded in Dicey's theory, data privacy law enforcement does not rely on law for effectiveness but needs to be accompanied by fair and consistent implementation of the law by bodies enforcing data privacy law.¹⁴³

¹³⁹ A V Dicey, *Introduction to the Study of the Law of the Constitution* (10th edn, Macmillan 1959) 193–198.

¹⁴⁰ Yemi Akinseye-George, *Constitutional Law and the Rule of Law in Nigeria* (MIJ Professional Publishers 2012) 44–47.

¹⁴¹ S Nnamodilim, I. Bolarinwa, M.T. Omidiora and O. Taiwo, 'Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment' (2024) 7 *International Journal of Law, Management and Humanities* 1278–1281.

¹⁴² Abiola Sanni, 'The Rule of Law and Regulatory Enforcement in Nigeria' (2018) 6 *Nigerian Journal of Public Law* 110–113.

¹⁴³ Oyewo Adebola, 'Data Protection, Regulatory Accountability and the Rule of Law in Nigeria' (2023) 11 *African*

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORK ON DATA PRIVACY IN NIGERIA

3.1 Overview of Nigeria's Legal Regime on Data Privacy

The regulatory landscape governing information privacy in Nigeria has developed gradually, based on constitutional guarantees and statutory advances. Notably, privacy rights are enshrined under section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended), which guarantees every citizen their right to privacy regarding their homes, correspondence, and telecommunications.¹⁴⁴ Historically, the country lacked a unified data privacy framework; instead, it relied on piecemeal regulations distributed in various statutes.¹⁴⁵ For example, the Cybercrimes Act of 2015 introduced mandates addressing data storage, protection against cyber threats, and the obligations of service providers.¹⁴⁶ Similarly, there were sector-specific regulations that came in the form of regulations issued by the CBN and the NCC that contained privacy obligations for banks and telecommunication providers, respectively.¹⁴⁷ However, the fragmented instruments failed to offer comprehensive protection or enforcement

Journal of Law and Human Rights 85–90.

¹⁴⁴ Constitution of the Federal Republic of Nigeria 1999 (as amended) s 37

¹⁴⁵ T Ilori, 'Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2023) 23(2) *African Human Rights*

Law Journal 899–923.

¹⁴⁶ Cybercrimes (Prohibition, Prevention, etc.) Act 2015 section 38.

¹⁴⁷ Central Bank of Nigeria (CBN) Consumer protection Framework, 2016 part iv; Nigerian Communications

Commission

(NCC) Consumer code of practice Regulations 2007 section 35.



clarity.¹⁴⁸

A major milestone occurred in 2019 when the National Information Technology Development Agency (NITDA) introduced the NDPR, establishing the nation's first structured rules for user consent, information management, and data subjects' rights.¹⁴⁹ Its introduction has raised compliance awareness, particularly among corporate organizations, and acted as an antecedent to legislation with stronger statutory force. Institutions have viewed obedience to the statute as a mere procedural formality, and regulators often lacked the resources to enforce adherence effectively.¹⁵⁰ Penalties imposed under the NDPR were restricted, and enforcement was not clear. This experience showed how the absence of a sound legislative basis for executive regulation could be limiting. The legal regime has also been shaped by Nigeria's international law and regional framework commitments. As it aligns with the African Union, Nigeria is bound to the Malabo Convention on Cyber Security and Personal Data Protection (2014) with an emphasis on contracting party obligations to protect personal data.¹⁵¹ Although the formal endorsement and domestication are sluggish, the existence of these frameworks has motivated Nigeria toward legislative reform.

Another issue inherent in the country's regulatory environment has been the widespread deficit in public knowledge about data rights. Their understanding regarding the extent of their rights under privacy law is usually very limited, and this lack of awareness has allowed corporations and state authorities to practice intrusive practices without strong

¹⁴⁸ J O Effoduh, 'Toward a Trustworthy and Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa' (2024) 6 *Data & Policy* e34.

¹⁴⁹ National Information Technology Development Agency, *Nigeria Data Protection Regulation 2019*.

¹⁵⁰ T Adegbite, 'NDPR Compliance Challenges in Nigeria' (2021) 15 *Journal of ICT Law* 78.

¹⁵¹ African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014.



resistance.¹⁵² Thus, for a strong legal framework to exist, there needs to be not only comprehensive laws but also careful public sensitization. Further, the existence of overlapping regulatory jurisdictions has been confusing in the past. NITDA, NCC, CBN, and other agencies all asserted jurisdiction over some aspects of data privacy, resulting in fragmented enforcement and reduced accountability.¹⁵³ Institutions were not held accountable, and inconsistent regulatory oversight was inevitable.¹⁵⁴ Failure of the old laws was brought into sharp relief as the digital economy of Nigeria grew by leaps and bounds. The advent of fintech, online marketplaces, and networking applications rendered personal data highly valuable, and at the same time, more vulnerable.¹⁵⁵

By 2023, stakeholders agreed that a comprehensive, statutory framework providing clarity, coherence, as well as administrative power was needed within the country. Consequently, the NDPA 2023 was passed; it represents a defining breakthrough in the evolution of the domestic data protection framework.¹⁵⁶

3.2 The Nigeria Data Protection Act 2023 (NDPA) (and applicable subsidiary instruments);

The principal statute functions as the cornerstone of the country's data privacy regime. It was passed to simplify and replace the NDPR 2019, which lacked the force of a

¹⁵² A Edgcumbe, J. Currie and S. McLennan, "'Potato Potato'? Disentangling De-Identification, Anonymization, And Pseudonymization in Data Protection Law' (2025) 12(1) *Journal of Law and the Biosciences* Isae029.

¹⁵³ O Adeyemi, 'Data Privacy Awareness in Nigeria' (2022) 3 *Lagos Law Review* 56.

¹⁵⁴ G W Greenleaf, 'International and Regional Commitments in African Data Privacy Laws' (2022) 46 *Computer Law and Security Review* 105743.

¹⁵⁵ A E Aimasiko, 'The Constitutionality of Fine Imposition Under the Nigeria Data Protection Act, 2023 and its Implications' (2024) *International Journal for Public Policy, Law and Development*.

¹⁵⁶ Nigeria Data Protection Act 2023 (NDPA 2023)

central authority.¹⁵⁷ The legislation creates a statutory structure aimed at safeguarding sensitive user details, aligning domestic policies with international paradigms such as the European Union's General Data Protection Regulation (GDPR).¹⁵⁸ Its passage was the first time the country had been equipped with a comprehensive, parliamentary-supported law specifically devoted to information security and individual confidentiality.¹⁵⁹ Among the core advancements introduced by the statute is instituting a centralized oversight authority known as the Nigeria Data Protection Commission (NDPC) in respect of data protection matters. This body has powers for enforcement, sanctions, and monitoring how the statute is applied across both state agencies and commercial entities.¹⁶⁰ The convergence of power under the NDPC both complements the regulatory fragmentation that has been the bane of the system in the past and adds to accountability.¹⁶¹ The NDPA 2023 has a wide description of personal data and sensitive personal data, the latter of which refers to health, religion, and biometrics, and has higher levels of protection.¹⁶² This classification is based on internationally accepted best practice and helps ensure that data in vulnerable classes is more directly

¹⁵⁷ M B Adisa and R Bashir, 'An Overview of the Nigeria Data Protection Act, 2023' <https://www.mondaq.com/nigeria/privacy-protection/1346676/an-overview-of-the-nigeria-data-protection-act-2023> accessed 3 February 2026 at 2:30 am.

¹⁵⁸ P C Aloamaka 'A Critical Analysis of the Nigeria Data Protection Act 2023' (2025) 2(1) *UCC Law Journal* 1–25

¹⁵⁹ O Babalola, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) *British Journal of Cyber Criminology* <https://www.pubtexto.com/journals/british-journal-of-cyber-criminology/fulltext/the-gdprstyled-nigeria-data-protection-act-2023-and-the-reverberations-of-a-legal-transplant> accessed 3 February 2026 at 2: 35am.

¹⁶⁰ A I Uwadima, 'The Digital Economy and Consumer Protection in Nigeria: A Legal Analysis of Data Privacy Laws under the Nigeria Data Protection Act 2023' (2025) *AUN Journal of Law*.

¹⁶¹ Dan Jerker Swantesson, *Private International Law and the Internet* (3rd edn, Kluwer Law International 2021)

112.

¹⁶² Nigeria Data protection Act sections 26, 65.

protected.¹⁶³

Consent is still a pillar of the NDPA.¹⁶⁴ The Act stipulates that the handling of private information can only be processed legally when supported by the explicit authorization of the individual provided the consent is freely, transparently, and unambiguously given.¹⁶⁵ Further, it recognizes particular rights for individuals, such as the privileges of data access, correction of inaccuracies, erasure of records, and data transferability.¹⁶⁶ These rights empower Nigerians to exercise enhanced autonomy regarding their online footprint.¹⁶⁷ The Act also puts heavy requirements on entities managing and processing data. The regulatory institutions must have in place robust technological and administrative safeguard to prevent data from being accessed, altered, or lost in an unauthorized manner. They also must keep records of processing activities and, in some cases, execute Data Protection Impact Assessments (DPIAs) before high-risk data processing operations.¹⁶⁸ These obligations are a quantum leap from the earlier NDPR framework.¹⁶⁹ In addition, in terms of enforcement, the NDPA 2023 has a major provision for imposing hefty penalties on violators. Fines are designed to be a deterrent, and target not just small enterprises but also large corporations whose activities impact millions of data subjects.¹⁷⁰ This method follows the rule that there should be practical

¹⁶³ P Hert and V Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the

Protection of Individuals?' (2016) *Computer Law & Security Review*.

¹⁶⁴ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013).

¹⁶⁵ Nigeria Data Protection Act 2023, section 25.

¹⁶⁶ Nigeria Data Protection Act 2023, sections 34–38.

¹⁶⁷ J E Cohen, 'What Privacy Is For' (2013) *Harvard Law Review*.

¹⁶⁸ C A Aloamaka, 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global

Norms' (2025) 4(2) *UCC Law Journal* 242.

¹⁶⁹ Olumide Babalola, 'Data Protection in Nigeria: The Journey So Far and the Road Ahead' (2020) *Gravitas Review*

of Business and Property Law.

¹⁷⁰ Nigeria Data Protection Act 2023, section 48.



repercussions from data privacy breaches to promote adherence.¹⁷¹ The NDPA also acknowledges the international nature of data privacy by regulating the provision of data overseas. Transfers are only allowed where there are sufficient levels of protection in the receiving country or where there are specific safeguards.¹⁷² This section conforms to norms of international standards and is necessary to build trust in transnational digital transactions.¹⁷³ Subsidiary measures are envisaged to become important instruments for the operation of the Act. These include guidelines, directives, and codes of practice published by the NDPC to clarify requirements for compliance.¹⁷⁴ Such instruments are the means to ensure that the broad principles of the NDPA are transformed into specific, enforceable standards in different sectors.¹⁷⁵ Importantly, the NDPA 2023 strikes a careful balance between the need to encourage innovation while safeguarding rights.¹⁷⁶ Forming a set of rules, it gives businesses legal certainty and reassures citizens that their data will not be used indiscriminately.¹⁷⁷ In a nutshell, the NDPA 2023 is a paradigm shift in the way Nigeria approaches data privacy. It brings the fragmented regime together into a comprehensive framework, it reinforces enforcement, and gives the protection of personal data statutory force.¹⁷⁸ As widely

¹⁷¹ A E Aimasiko, 'The Constitutionality of Fine Imposition Under the Nigeria Data Protection Act, 2023 and its

Implications' (2024) *International Journal for Public Policy, Law and Development*.

¹⁷² Nigeria Data Protection Act 2023, section 41.

¹⁷³ P C Aloamaka, 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global

Norms' (2025) 4(2) *UCC Law Journal* 242.

¹⁷⁴ Nigeria Data Protection Act 2023, section 61.

¹⁷⁵ A B Makulilo, 'Data Protection in Africa: A Comparative Perspective' (2016) *African Journal of Information and Communication*.

¹⁷⁶ A I Uwadinma, 'The Digital Economy and Consumer Protection in Nigeria: A Legal Analysis of Data Privacy

Laws under the Nigeria Data Protection Act 2023' (2025) *AUN Journal of Law*.

¹⁷⁷ Christopher Kuner, 'The Internet and the Global Reach of EU Law' (2017) *Columbia Journal of European Law*.

¹⁷⁸ Olumide Babalola, 'Data Protection in Nigeria: The Journey So Far and the Road Ahead' (2020) *Gravitas Review*



acknowledged in data protection scholarship, "data protection is not an obstacle to innovation; it is the foundation on which sustainable innovation must rest."¹⁷⁹

3.3 Other Relevant Laws and Regulations (e.g., Cybercrimes Act, NCC Regulations, CBN Guidelines)

3.3.1 Constitution of the Federal Republic of Nigeria 1999 (As Amended)

Apart from NDPA 2023, data protection framework is underpinned by a suite of other statutes and regulatory instruments that overlap with personal data protection. No matter how one evaluates data privacy, its historical development within the country originates from constitutional guarantees safeguarded under the Constitution.¹⁸⁰ By elevating the right to privacy to a fundamental right, Section 37 serves as the primary constitutional bedrock for safeguarding of personal data across Nigeria. Also, by placing the right to privacy on the pedestal of a fundamental right, it automatically attaches to it the highest level of protection in the land.¹⁸¹ The provision has also been interpreted expansively by the courts. In *Nwali v Ebonyi State Independent Electoral Commission (EBSIEC)*¹⁸², The Appeal Court adopted an expansive reading of privacy rights, holding that it encompasses virtually every facet of human existence. Even though the judiciary abstained from explicitly using the expression "data protection" directly, its judgment is widely regarded as laying an important doctrinal foundation for the recognition of informational privacy under Nigerian law.¹⁸³

of Business and Property Law.

¹⁷⁹ L A Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014).

¹⁸⁰ Constitution of the Federal Republic of Nigeria 1999 (as amended).

¹⁸¹ In *El-Rufai V. Senate of National Assembly (2016)1 NWLR pt 1494 at page 534*, the court held that "owing to its

peculiar nature, and being a constitutional right, a fundamental right is certainly a right which stands above

ordinary laws of the land".

¹⁸² (2014) LPELR-23682(CA).

¹⁸³ Olumide Babalola, *Data Protection Law and Practice in Nigeria* (Law Lords 2020) 13.



While the historical growth of data privacy regimes is rooted within general privacy protection, recent developments indicate a paradigm shift towards a new legal regime that governs how personal data is gathered, handled, and utilized.¹⁸⁴ Modern data protection law is no longer just about confidentiality but also the regulation of data processing activities and institutions.¹⁸⁵ Moreover, section 37 does not specifically address fundamental data privacy tenets, including fair and lawful data handling, purpose limitation, and transparency.¹⁸⁶ This underscores the limitations and shortcomings of constitutional privacy law in dealing with modern issues surrounding digital data governance.¹⁸⁷ Nonetheless, informational privacy remains a fundamental normative basis for the law, especially before the promulgation of the NDP 2023. It therefore represents an important starting point, though insufficient on its own to regulate contemporary data processing activities.¹⁸⁸ Apart from the general and sectoral regulatory frameworks, several laws in Nigeria protect personal data in particular areas.¹⁸⁹

3.3.2 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 as amended 2024

A foundational piece of legislation within Nigeria impacting data protection is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. This statute is chiefly designed to prevent cybercrime; it is equally vital in combating data abuse, identity theft, and unlawful access to electronic communication.¹⁹⁰ The Act mandates that telecom

¹⁸⁴ Graham Greenleaf, *Asian Data Privacy Laws* (OUP 2014) 23.

¹⁸⁵ A Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 56.

¹⁸⁶ Olumide Babalola, *Data Protection Law and Practice in Nigeria* (Law Lords 2020) 15.

¹⁸⁷ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP 2013) 78.

¹⁸⁸ A Bygrave, *Data Privacy law: An International perspective* (OUP 2014) 60.

¹⁸⁹ P C Aloamaka 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global

Norms' (2025) 4(2) *UCC Law Journal* 242.

¹⁹⁰ O Adeboyejo 'Cybersecurity, Privacy and Legal Protection of Personal Data in Nigeria' (2020) 12 *African*



operators preserve user data on subscribers for two years, which can only be released under certain circumstances, including when ordered by the court.¹⁹¹ Furthermore, the statute specifies that in the exercise of duties pursuant to section 38, regard must be had to the privacy rights of an individual and necessitates proper protection of the secrecy of any information collected, managed, or accessed.¹⁹² Additionally, it criminalizes the interception of electronic communication without authorization, an action that may occur during law enforcement inquiries lacking judicial approval.¹⁹³

However, these provisions have generated concerns regarding the potential tension between cybersecurity enforcement and the preservation of individual privacy rights. Notwithstanding the rationales presented under the guise of national security, the Act has been accused of possible government excesses that may compromise the safety of private information and create a conflict of interest in ensuring cybersecurity in Nigeria and safeguarding an inherent human right.¹⁹⁴ The Act has been accused of lacking independent oversight, potentially resulting in the abuse of private records and consequently fostering a lack of trust in online services in Nigeria.¹⁹⁵

3.3.3 Child's Right Act 2003

This 2003 statute reinforces the constitutional privacy entitlements of minors. It characterizes a minor as anyone below eighteen years old, explicitly establishing and safeguarding their fundamental privileges. Pursuant to Section 8, every minor, whether

Journal of Law and Technology 56.

¹⁹¹ Cybercrimes (Prohibition, Prevention, etc.) Act 2015 section 37–38

¹⁹² Cybercrimes (Prohibition, Prevention, etc.) Act 2015 section 38(5)

¹⁹³ Cybercrimes (Prohibition, Prevention, etc.) Act 2015 section 33

¹⁹⁴ A Chukwumerije, 'Privacy versus Security: Cybercrime Laws in Nigeria' (2021) 9 *African Journal of International and Comparative Law* 77

¹⁹⁵ B van der Sloot, 'Surveillance, Cybercrime and the Limits of Privacy' (2017) 3 *International Journal of Law and*

Information Technology 101.



adopted¹⁹⁶ or fostered¹⁹⁷, is entitled to privacy, which includes the nondisclosure of personal information, under parental guidance, especially considering how vulnerable children are in matters concerning digital and educational settings.¹⁹⁸ The Act also expressly protects the privacy interests of minors across all phases of the juvenile justice system¹⁹⁹ and prohibits any publications that can reveal the identity of the child²⁰⁰. According to legal writers, this law places a responsibility on individuals and institutions to protect a child's data and serves as a foundation for Nigeria's data protection regime.²⁰¹

3.3.4 The Credit Reporting Act 2017

The Act regulates access to credit information within the Nigerian financial sector alongside connected issues. It oversees how credit information is collected, maintained, and disseminated, requiring confidentiality from financial institutions and credit bureaus, and empowers consumers to review, amend, and request corrections to their personal credit histories.²⁰² Section 7(1) of the Credit Reporting Act stipulates that an entity utilizing credit data is restricted to requesting records from a bureau solely for authorized purposes outlined by the law.²⁰³ Also, section 6(1) of the Act lists certain

¹⁹⁶ Section 142(9) of Child's Rights Act 2003

¹⁹⁷ Ibid Section 112(9)

¹⁹⁸ O A Adediran, *Child Privacy and Digital Rights in Nigeria: Legal Obligations and Protections* (2023) 14 *Africa Journal of Law and Technology* 112.

¹⁹⁹ Section 205(1) of Child's Right Act 2003.

²⁰⁰ Child's Right Act 2003 section 205(2).

²⁰¹ F N Okonkwo, 'Children's Privacy and Data Protection in Nigeria: Legal and Institutional Responsibilities'

(2022) 8 *Nigerian Journal of Law and Technology* 101.

²⁰² Felicia Nwanne Monye, Ndubuisi Nwafor and Benjamin Mukoro, 'Appraisal of the Nigerian Credit Reporting

Act 2017' (2020) 64(2) *Journal of African Law* 229.

²⁰³ For example, when considering a person's application for credit or a person's qualification to act as a guarantor

for any credit; reviewing, renewing restructuring or monitoring of existing credit facilities; carrying out employment checks on current or prospective employees etc - See section 7(2) of the Credit Reporting Act.

mandatory obligations of a credit bureau, particularly regarding data integrity, confidentiality, security safeguards, information quality and accuracy, and use limitation. Furthermore, Part V - section 9(1) of the Act states that “Except as this Act provides otherwise, Data Subjects shall have the right to the privacy, confidentiality and protection of their credit information”. This law is important in ensuring financial privacy, combating identity theft, and fostering confidence within the country’s financial environment.²⁰⁴

3.3.5 The Freedom of Information Act 2011

The Freedom of Information Act 2011 controls how state entities disseminate individual data. Despite not being formally classified as data protection legislation, it outlines distinct regulations for securing individual data. Personal information of citizens is only disclosed with the consent of the person concerned or with statutory backing, which enhances the preservation of individual confidentiality.²⁰⁵ Subject to specific exceptions²⁰⁶ Section 14 of the FOI Act mandates that public institutions deny access to private records. Additionally, public institutions have the discretionary authority under Section 16 of the FOI Act to reject requests pertaining to specific privileged information, including attorney-client privilege, health worker-client privilege, journalistic confidentiality privilege, and any other legally recognized professional privileges. However, this Act's reach is restricted to controlling the retrieval of data and records

²⁰⁴ Kubi Udofia, *A Critical Analysis of Credit Information Sharing Under Nigeria’s Credit Reporting Act 2017* (SSRN Paper, 3 October 2017) <https://ssrn.com/abstract=3047188> accessed 1 April 2026 at 4:05 am.

²⁰⁵ Freedom of Information Act 2011, section 14, section 16.

²⁰⁶ If the individual to whom such information relates consents to the disclosure or the information if made publicly available, see section 14(2) of the freedom act 2011.

stored within state agencies.

3.3.6 The National Identity Management Commission (NIMC) Act of 2007

The National Identity Management Commission (NIMC) Act of 2007 regulates entry to the individual identification data stored within the National Identity Database, thereby seeking to balance administrative efficiency with defending individual privacy rights.²⁰⁷

Section 14 expressly authorizes the formation of a national identity database to store the enrolled data of nationals and foreign residents classified as eligible enrollees²⁰⁸ under the Act. Section 26 provides that both individuals and corporate entities are barred from retrieving records kept in the database without authorization. The prohibition has specific exceptions, which are where the request is granted following the approval of the registered person, or when access to the information is made necessary for public interest, national security, or for crime prevention and investigative efforts or for alternative grounds under the Act.²⁰⁹

3.3.7 Sector-specific laws on Data privacy

3.3.7.1 Nigerian Communications Act²¹⁰ 2003

In furtherance of its obligation under Section 70, the NCC has promulgated various regulations that are designed to govern the protection of the privacy of subscriber data in the telecommunication industry in Nigeria. The Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 outline a

²⁰⁷ National Identity Management Commission Act 2007, section 26.

²⁰⁸ Any individual who is a citizen of Nigeria; any individual, regardless of citizenship status, who is lawfully and permanently residing in Nigeria; and any non-citizen of Nigeria who is lawfully residing in Nigeria for a period

of Two years or longer: Refer to the National Identity Management Commission Act of 2007's Sections 16(a)–(c).

²⁰⁹ National Identity Management Commission Act of 2007 section 26.

²¹⁰ Nigerian Communications Act 2003, CAP N97 LFN 2010



complete regime for registration of telephone subscribers, creation, management, and control of the centralized subscriber database, as well as the incorporation of essential data privacy standards which must be observed by the network service providers.²¹¹ In addition, the Nigerian Communications Commission (Consumer Code of Practice) Regulations 2024 regulate the privacy of consumer data in the telecommunications industry in Nigeria²¹². These regulations apply to all subscribers without discrimination of any kind, regardless of their citizenship status. Furthermore, the NCC established the Lawful Interception of Communications Regulations 2019, which greatly enhances the investigative monitoring reach of public authorities by enabling designated law enforcement agencies, pursuant to Regulation 4, to monitor communications through NCC licensees in Nigeria or elsewhere outside Nigeria, provided that certain criteria are met, among which are situations when monitoring is done either with or without warrants.²¹³

3.3.7.2 Regulatory frameworks issued by the Central Bank of Nigeria

Specialized privacy rules have been institutionalized throughout the financial sector by means of policies enacted by the Central Bank of Nigeria (CBN).²¹⁴ For instance, the CBN Consumer Protection Framework 2016 requires that commercial institutions secure customer information meticulously, and the CBN Risk-Based Cybersecurity Framework places data security at the core of financial stability²¹⁵. The guidelines focus on risk assessment, encryption, staff training, and the development of internal policies

²¹¹ Section 2 of the NCC Registration Regulations

²¹² See the schedule to the NCC Consumer Code of Practice Regulations. Particularly, part VI of the Model Consumer Code of Practice regulation 45.

²¹³ Eniye Emilia Ogbekor, 'Privacy and Data Protection in Digital Age: Does Nigeria Need a Data Protection Law?' (n.d.).

²¹⁴ Central Bank of Nigeria, *Consumer Protection Framework* (2016).

²¹⁵ A E Aimasiko, 'The Constitutionality of Fine Imposition Under the Nigeria Data Protection Act, 2023 and its

Implications' (2024) *International Journal for Public Policy, Law and Development*.



for the governance of data as integral components for an effective privacy and security strategy.²¹⁶ Such measures are especially important in the context of a digital age banking system, where financial data is particularly vulnerable.²¹⁷ The apex bank, in collaboration with the Bankers' Committee, launched the BVN project in February 2014.²¹⁸ This initiative by the CBN was aimed at promoting the protection, efficiency, and reliability of the country's payment structure. BVN provides a unique identity for the customers of banks in Nigeria. Further, the CBN issued the BVN Framework, one of whose roles is to provide mechanisms for ensuring the privacy of the data on bank customers under the BVN.²¹⁹

3.3.7.3 National Health Act 2014 (NHA)

The National Health Act of 2014 governs the healthcare system and the administration of medical services in Nigeria.²²⁰ The Act considers all information regarding individuals who access health services confidential and its disclosure forbidden except under certain circumstances.²²¹ It includes instances when the patient formally agrees to the release of his or her medical records, when there is legal compulsion for the same, when dealing with minor children or people who cannot provide consent due to mental infirmity, or when withholding information poses public health dangers. Comparable confidentiality obligations also exist within the healthcare sector, where patient

²¹⁶ Central Bank of Nigeria, *Risk Based Cybersecurity Framework and Guidelines for Deposit Money Banks and*

Payment Service Providers in Nigeria (2018), parts 4–6, 10–12.

²¹⁷ O A Adegbite, 'Data Protection and Cybersecurity Challenges in Nigerian Digital Banking' (2021) 15(2) *Journal*

of Banking and Financial Law 45.

²¹⁸ The BVN number can be classified as pseudonymous personal data.

²¹⁹ Paragraph (1.8) of the BVN framework

²²⁰ S Olarinde, I Bamidele and O Ajigboye, *Imperatives of Access to Health Care in Nigeria under the National*

Health Act, 2014 (2023) 4 *University of Ibadan Law Journal* (discussing the legislative framework and objectives of the Act)

²²¹ Damola Obisesan, 'Health Data Privacy in Nigeria: The NHA and NDPR' (2024).



information is particularly sensitive.²²² While there is no Health Information Privacy Act (HIPA) in place in Nigeria, there are confidentiality provisions in guidelines issued by the Federal Ministry of Health and in professional codes of conduct for health practitioners.²²³ Within the healthcare administration, data security for patients is reinforced by the Act, which prescribes the criteria for information sharing.²²⁴

3.3.7.4 HIV/AIDS (Anti-Discrimination) Act in 2014

To secure the sensitive information of affected patients, the National Assembly passed the HIV/AIDS (Anti-Discrimination) Act in 2014.²²⁵ This is a very important area due to the sensitivity of the medical records, but enforcement is still low.²²⁶ Section 13 states that (1) every individual diagnosed with HIV and AIDS is entitled to confidentiality regarding information about their health status. (2) Violation of the provision constitutes a punishable crime carrying a fine of not less than five hundred thousand naira for a person, or one million naira for a corporate entity; or imprisonment of not more than two years, or both.²²⁷ It establishes the rule on confidentiality by banning the unauthorized release of an individual's HIV status unless permission is granted, except in limited, legally recognized circumstances such as a court order²²⁸ for the protection of a sexual partner, where the patient refuses to disclose for medical necessity or

²²² K C Anyanwu, U M Mbanaso, T K Anyachebelu and S E Chaku, 'Assessment of Compliance with Data Protection and Privacy Regulations in the Nigerian Healthcare Sector' (2025) 1(1) *SIAR Global Journal of*

Computer, Information & Library Science.

²²³ I Shehu and S R Bello, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria' (2022)

Journal of Law, Policy and Globalization.

²²⁴ National Health Act, 2014. Sections 26 and 29

²²⁵ O C Genevieve, 'Confidentiality and Public Health: An Examination of Legal and Ethical Frameworks Governing Doctor's Duty to Disclose Serious Health Conditions in Nigeria' (2025) *FUNAID Law Review Projects.*

²²⁶ O I Ottah and E S Imoisi, 'An Appraisal of the Legal Framework for Data Security Protection for Health Institutions in Nigeria' (2025) 16(2) *Journal of Current Research and Review.*

²²⁷ HIV and AIDS (Anti-Discrimination) Act, 2014

²²⁸ Section 11 of the HIV and AIDS (Anti-Discrimination) Act, 2014



treatment, or as expressly permitted by law. In all such cases, disclosure must be limited to what is necessary, executed with genuine intent, while confidentiality is maintained as far as possible to balance privacy rights with public health concerns.²²⁹

Collectively, these statutes establish a mosaic of sector-specific personal privacy protection provisions that are supplemented by the NDPA of 2023, the NCC regulations, and the CBN guidelines.²³⁰ However, scholars emphasize the need to harmonize these provisions due to the fragmentation and overlap of the provisions in order to create a unified and all-encompassing personal privacy framework in all sectors of the economy.²³¹

In addition, it is worth highlighting the growing appreciation within certain corporate governance codes and industry-specific compliance guidance that data security is embedded within fiduciary duty. Privacy must become a part of governance structures; organizations must implement internal policies, designate data protection officers, and establish security protocols. However, these different frameworks are frequently run in silos, which leads to duplication and inconsistency. The lack of a coherent enforcement bedrock makes conformance uneven and, many times, voluntary. Traditionally, this has impeded the credibility of Nigeria's data protection regime.²³²

Without well-defined roles, organizations can end up with competing mandates, and

²²⁹ Orenike Folayan and Brandon Brown, 'HIV, Stigma, and Human Rights in Nigeria' (2015) *BMC International Health and Human Rights* 15(14).

²³⁰ N C Ezech, 'National Identity Management and Privacy in Nigeria: Balancing Access and Confidentiality' (2023)

10 *Journal of Nigerian Law and Policy* 78.

²³¹ F Obioha, 'Harmonising Data Protection Laws in Nigeria: Challenges and Prospects' (2024) 11 *Journal of African Legal Studies* 67.

²³² E A Ukwandu and others, *Cyber Security in the Emerging World of Smart Everything* (2021).

regulators can duplicate efforts rather than work together. Harmonization of these laws is therefore very important for effectiveness.²³³ Ultimately, the efficacy of Nigeria's data safety regime depends not only on the strength of the NDPA 2023 but equally upon the coherence, coordination, and enforcement consistency of the broader network of supporting statutes and regulatory instruments that give practical effect to its provisions²³⁴. For example, the banking sector has specific risks that differ from those of the telecommunications sector or healthcare, and has appropriately specific responses available through sectoral guidance. As one legal commentator put it: "the efficacy of a data protection regime is not solely contingent on the potency of the core statute but on the consistency of all the surrounding laws and regulations that provide practical effectiveness to the core statute"²³⁵.

3.4 Comparative Analysis of Selected Jurisdictions (e.g., EU-GDPR, South Africa's Personal Information Protection and Electronic Documents Act (POPIA)).

Although such a comparison has been provided, it would serve as a useful point of reference for Nigeria's data privacy regime.²³⁶ It remains a useful analytical reference point for evaluating the effectiveness and development trajectory of Nigeria's data protection regime, particularly given the interdependence of digital transactions across jurisdictions worldwide.²³⁷ The European Union's General Data Protection Regulation

²³³ M A Bouke, and others, 'African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions' (2023).

²³⁴ Olumide Babalola, *Nigeria's Data Protection Legal and Institutional Model: An Overview* (2021) 12(1) International Data Privacy Law.

²³⁵ I Shehu and S R Bello, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria' (2022) *Journal of Law, Policy and Globalization*.

²³⁶ Olumide Babalola, 'The EU GDPR and Nigeria's NDPR: A Comparative Analysis' (2021) 4(4) *Journal of Data Protection & Privacy* 372.

²³⁷ A E Aimasiko, 'The Constitutionality of Fine Imposition under the Nigeria Data Protection Act 2023 and Its Implications' (2024) *International Journal for Public Policy, Law and Development*.

(GDPR) is considered the gold standard for data protection, imposing strict requirements on controllers and processors and offering strong rights to data subjects.²³⁸ Its extraterritorial extension has influenced legislative reforms worldwide, including Nigeria's NDPA.²³⁹ The GDPR focuses on principles that include lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability.²⁴⁰ It redefined the meaning of lawful processing of personal data; attached stricter measures to the processing of sensitive personal data, and expanded its territorial scope to apply to non-EU businesses in certain circumstances; introduced higher accountability standards; more severe penalties for non-compliance; more stringent requirements for broader data transfers, and now requires companies to appoint data protection officers.²⁴¹

These Principles ensure that personal data processing is governed by structured legal safeguards rather than arbitrary institutional discretion.²⁴² The influence of the European model is evident in many of the principles incorporated by Nigeria's NDPA 2023, particularly those relating to lawful processing, transparency obligations, and accountability mechanisms.²⁴³ Furthermore, the GDPR has the benefit of solid institutional enforcement in the form of Data Protection Authorities in EU member

²³⁸ O Ekpo and O Aiyetan, 'A Comparative Analysis of Nigeria's NDPA and the EU's GDPR' in *Proceedings of the*

2024 International Conference on Information Technology & Data Analytics (ACM 2024).

²³⁹ L A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014).

²⁴⁰ Adekunle Adewumi, 'Adequate Protection: An Analysis of Nigeria's Data Protection Laws within an Emerging

Framework' (LLM thesis, University of Victoria 2022).

²⁴¹ Christopher Kuner, L A Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2024).

²⁴² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data

Protection Regulation) art 5.

²⁴³ Graham Greenleaf, *Global Data Privacy Laws 2023: Despite COVID Delays, 162 Laws Show GDPR Dominance* (Privacy Laws & Business International Report 2023).



states, like the European Data Protection Board.²⁴⁴ In contrast, Nigeria is only at its formative stage of consolidating its enforcement architecture under the Nigeria Data Protection Commission.²⁴⁵

South Africa's Protection of Personal Information Act (POPIA) provides another instructive comparative framework²⁴⁶. Although enacted in 2013 became fully operational from 2021, and it establishes a fully-fledged data protection regime that is tailored to South Africa's constitutional and socio-economic environment.²⁴⁷ Like the GDPR, POPIA embeds enforceable data subject rights alongside clearly defined compliance obligations for controllers.²⁴⁸ It also set up the Information Regulator, a specialized supervisory regulator tasked with monitoring and enforcing compliance.²⁴⁹

An important advantage of POPIA is that it is embedded in South African constitutional jurisprudence, in particular the right to privacy enshrined under Section 14 of the South African Constitution.²⁵⁰ This constitutional basis has created solid judicial engagement with informational privacy rights and has enhanced the legitimacy of the country's data protection enforcement framework²⁵¹. Nigeria has a similar constitutional underpinning

²⁴⁴ Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017).

²⁴⁵ I A Abdullahi, 'An Appraisal of the Institutional Framework under the Nigeria Data Protection Act 2023' (2024)

Nigerian Journal of Public Law.

²⁴⁶ H Ncube, 'Data Protection in Africa: A Comparative Perspective on the Protection of Personal Information Act'

(2021) *African Human Rights Law Journal*.

²⁴⁷ Protection of Personal Information Act 4 of 2013 (South Africa).

²⁴⁸ United Nations Conference on Trade and Development (UNCTAD), *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (UNCTAD 2016).

²⁴⁹ P Plantinga and others, 'Responsible Artificial Intelligence in Africa: Towards Policy Learning' (2024) 6 *Data & Policy* e23.

²⁵⁰ Donrich Thaladar, 'The Protection of Personal Information Act and Constitutional Privacy in South Africa' (2020)

South African Journal on Human Rights 341.

²⁵¹ Michael Birnhack, 'Constitutional Privacy and Data Protection in Comparative Perspective: Lessons



in section 37 of the Constitution of the Federal Republic of Nigeria, 1999.²⁵² However, judicial interpretation in Nigeria has not yet attained the sustained doctrinal development in the field of data privacy.²⁵³

Another comparative lesson is related to public awareness and a compliance culture. In the EU, the GDPR has evolved into a routine component of corporate governance and regulatory compliance, and in South Africa,²⁵⁴ POPIA has spawned important education initiatives and institutional awareness campaigns within South Africa.²⁵⁵ By comparison, Nigerians have low-level knowledge of data protection because awareness of the laws in place is limited, and it continues to constrain the practical effectiveness of the country's legal framework.²⁵⁶

In addition, the GDPR and POPIA make explicit provisions for the transfer of data across borders, either through adequacy decisions or through robust contractual protections.²⁵⁷ The enforcement of such rules requires considerable institutional capacity and regulatory coordination, which is a problem in Nigeria; however, similar provisions are found in the NDPA 2023.²⁵⁸ Both GDPR and POPIA also emphasize the

from South

Africa' (2021) *International Data Privacy Law* 1.

²⁵² Constitution of the Federal Republic of Nigeria 1999, section 37.

²⁵³ A E Aimasiko, 'The Constitutionality of Fine Imposition under the Nigeria Data Protection Act 2023 and Its

Implications' (2024) *International Journal for Public Policy, Law and Development*.

²⁵⁴ K Kopp and M Schreiner, 'GDPR Implementation and Corporate Compliance in Europe' (2024) *Journal of Data*

Protection & Privacy 145.

²⁵⁵ L Mahlangu, 'Public Awareness and POPIA Compliance in South Africa' (2025) *South African Law Journal* 78.

²⁵⁶ Chidi Okereke and Ifunanya Eze, 'Data Protection Awareness and Compliance Challenges in Nigeria's Digital

Economy' (2023) *Nigerian Journal of Law, Technology & Innovation* 5(2) 97.

²⁵⁷ Protection of Personal Information Act 4 of 2013 (South Africa) section 72; Regulation (EU) 2016/679 (General

Data Protection Regulation) article 45–46.

²⁵⁸ Nigeria Data Protection Act 2023, sections 41–43

importance of accountability through mechanisms such as Data Protection Impact Assessments (DPIAs).²⁵⁹ These mechanisms provide for organizations to assess risks before engaging in high-risk data processing activities. Nigeria's NDPA includes DPIA requirements, but faces the issues of institutional oversight capacity and the development of stronger corporate adherence.²⁶⁰

A rather significant comparative insight is the penalties for violations. Penalties under the GDPR can reach up to 4% of global annual turnover or up to 20 million euros²⁶¹, whichever is higher, guaranteeing a truly dissuasive penalty. POPIA also imposes heavy penalties, including criminal liability for serious violations.²⁶² Nigeria's NDPA 2023 has instituted harsher penalties than those previously available under the NDPR 2019²⁶³, but has yet to reach the level of deterrence offered by GDPR framework.²⁶⁴

Nigeria can also draw useful lessons from collaborative enforcement structures developed within the European Union, where data protection authorities work together through the European Data Protection Board (EDPB) to coordinate regulatory action.²⁶⁵ Regional cooperation in Africa is still developing, but Nigeria could gain by taking a leading role in cross-border cooperation, especially under the African Continental Free Trade Area (AfCFTA).²⁶⁶ As one scholar has noted: "Comparative law is not imitation

²⁵⁹ Regulation (EU) 2016/679 (General Data Protection Regulation) article 35; Protection of Personal Information

Act 4 of 2013 (South Africa) ss 4(1)(b), 19.

²⁶⁰ Chinwe Okafor, 'Assessing Nigeria's Data Protection Regime Post-NDPA 2023' (2024) *African Journal of Law and Technology*.

²⁶¹ Regulation (EU) 2016/679 (General Data Protection Regulation) article 83(5).

²⁶² Protection of Personal Information Act 4 of 2013 (South Africa) sections 100–109.

²⁶³ Nigeria Data Protection Act 2023, sections 48–49

²⁶⁴ Uchenna Jerome Orji, 'Nigeria's Data Protection Act 2023: Context, Content and Implications' (2024) *Computer Law & Security Review*.

²⁶⁵ Regulation (EU) 2016/679 (General Data Protection Regulation) articles 63–65;

²⁶⁶ Babatunde Faturoti and Ibrahim Juma, 'Enforcing Data Privacy in Kenya and Nigeria: Towards an



but adaptation; the challenge for Nigeria is to learn from global standards while devising solutions appropriate to its local realities."²⁶⁷

3.5 Regional Data Protection Frameworks: The ECOWAS Supplementary Act and the African Union Malabo Convention

In addition to global regulatory influences like the EU GDPR and POPIA in South Africa, regional regulatory frameworks in West Africa and within the AU have also played a critical role in influencing Nigeria's emerging data protection landscape.²⁶⁸

In 2007, the Heads of State and Government of ECOWAS adopted Supplementary Act A/SA.1/01/07 on the harmonization of policies and the regulatory framework for the ICT sector in the region.²⁶⁹ Acknowledging the interconnection between ICT development and the management of personal data, ECOWAS further adopted Supplementary Act A/SA.1/01/10 on Personal Data Protection in February 2010 in Abuja.²⁷⁰ The Act is a legal framework that regulates the collection, processing, transmission, storage, and utilization of personal data by both government and private bodies within the Member States. nwali

Before the introduction of the ECOWAS Supplementary Act for the Protection of Personal Data, not many Member States had established laws for data protection at the national level, outside regional initiatives to coordinate such activities.²⁷¹ With the introduction of the Supplementary Act, however, a few more Member States have put in

African

Approach to Regulatory Practice' (2025) *International Review of Law, Computers and Technology* 1.

²⁶⁷ Uchenna Jerome Orji, *Digital Rights and Cybersecurity in Nigeria* (IGI Global 2018) 142.

²⁶⁸ Olumide Babalola, *Data Protection Compliance in Nigeria* (Snaap Press 2020).

²⁶⁹ ECOWAS Supplementary Act A/SA.1/01/07 relating to the harmonization of policies and the regulatory framework for the ICT sector.

²⁷⁰ ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010).

²⁷¹ A B Makulilo, 'African Data Privacy Laws: A Comparative Perspective' (2016) 6 *International Data Privacy Law*.



place legislative measures that partially meet the requirements of the regional legal instrument.²⁷² Nonetheless, the existence of national legislation does not guarantee that the provisions made by the regional legal document are completely observed. For instance, one of the key demands made by the ECOWAS framework is that Member States put in place an Independent Data Protection Authority, which is independent, immune, and confidential.²⁷³

In Nigeria, despite the ECOWAS Supplementary Act being occasionally cited as one of the instruments that may have contributed to national data protection policy formulation as a result of regional considerations, it has never been domesticated as part of Nigeria's statutory provisions.²⁷⁴ Therefore, the ECOWAS Supplementary Act lacks any enforceable force under the law in Nigeria, pursuant to section 12 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).²⁷⁵

The African Union Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention) is yet another important regional mechanism at the continental level that seeks to harmonize cybersecurity and personal data protection regulations in Africa.²⁷⁶ The Convention was adopted by the African Union Assembly in June 2014 to create an all-inclusive legal regime for e-transactions, cybersecurity governance, and personal data protection within the Member States.²⁷⁷

²⁷² ECOWAS Supplementary Act A/SA.1/01/10

²⁷³ Ibid. Article 22.

²⁷⁴ Constitution of the Federal Republic of Nigeria 1999 (as amended) s 12; *Abacha v Fawehinmi* (2000) 6 NWLR (Pt 660) 228.

²⁷⁵ I Oraegbunam and Emeka Christian Iroanya, 'Section 12 of the 1999 Constitution of Nigeria and Treaty Implementation: A Legal Critique' (2023) 5(2) *International Review of Law and Jurisprudence*

²⁷⁶ A B Makulilo, 'The African Union Convention on Cyber Security and Personal Data Protection: A Missed Opportunity?' (2016) 7 *Computer Law Review International*.

²⁷⁷ African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) AU

Just like the Council of Europe's Convention 108, the Malabo Convention provides for a treaty-based regime on how personal data is processed by individuals and entities such as organizations and public authorities.²⁷⁸ This regime is complemented by fundamental principles similar to those provided for under GDPR.²⁷⁹ In addition, Member States are required to develop national regimes that enhance the protection of fundamental human rights while ensuring the safe transfer of personal data within the continent.²⁸⁰

Notwithstanding its significance within the developing digital governance framework in Africa, the Malabo Convention came into effect on June 8, 2023, after attaining the minimum of fifteen ratifications required by Article 36 of the convention.²⁸¹ Although Nigeria has signed the convention on 23rd January 2024, but is yet to ratify it therefore, it is not legally bound by the provisions.²⁸² The influence of such an international instrument can be observed indirectly through Nigeria's developing regulatory environment²⁸³. As mentioned earlier, the Implementation Framework of the NDPR encourages the use of international cooperation measures and regional laws in bridging

Doc

EX.CL/846(XXV). (Executive Council Document No. 846 from the 25th session)

²⁷⁸ Article 9 of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)

(adopted 27 June 2014), African Union.

²⁷⁹ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 112–138.

²⁸⁰ W H Kruskal and P G B Berger, 'Cross-Border Data Flows and National Data Protection Frameworks: Comparative Perspectives' (2022) 28 Computer Law & Security Review 105469.

²⁸¹ Michalsons, *AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)* (updated

2023) [https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-](https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281)

[convention/65281](https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281) accessed 5 April 2026 at 8:17 am.

²⁸² Horizon, *Africa's Cybersecurity Treaty Enters into Force* (EU CyberDirect, 2023)

https://eucyberdirect.eu/blog/africa-s-cybersecurity-treaty-enters-into-force?utm_source=chatgpt.com accessed 5

April 2026 at 8:23 am.

²⁸³ Nigeria Data Protection Regulation 2019: Implementation Framework (NITDA, November 2020) section 16.



interpretation gaps that arise in relation to data protection regulation.²⁸⁴

Thus, although both the ECOWAS Supplementary Act and the Malabo Convention cannot be relied upon as instruments with direct enforceability within the domestic legal context of Nigeria at the moment, both instruments nonetheless hold great significance in the regional harmonization process of data protection regulation in West Africa.²⁸⁵

3.6. Enforcement and Institutional Roles

Given the importance of the data privacy regime, the institutions of enforcement are extremely important. In Nigeria, the Nigeria Data Protection Commission (NDPC) is the central body that has been created under the NDPA 2023²⁸⁶ to ensure compliance, regulate controllers and processors, and impose sanctions for non-compliance. The institutional centralization is a break from the fragmented regime of the past.²⁸⁷ The NDPC has powers to inquire into complaints, audit, issue compliance directions, and work with overseas regulators.²⁸⁸ Its importance lies in the ability of the Regulation to translate statutory provisions of the NDPA into concrete protections for data subjects.²⁸⁹ Before the NDPA, responsibilities relating to enforcement were spread across the NITDA, NCC, CBN, and other sectoral regulators. Transference of control of NDPC is a big step Nigeria has taken toward streamlining enforcement²⁹⁰

²⁸⁴ Ibid section 16.

²⁸⁵ O B Adelakun, 'The African Union Convention on Cyber Security and Personal Data Protection – Prospects and Challenges' (2017) 61 *Journal of African Law* 123.

²⁸⁶ Section 4 of the Nigeria Data Protection Act 2023 section

²⁸⁷ E A Ukwandu and others, *Cyber Security in the Emerging World of Smart Everything* (2021).

²⁸⁸ Section 5 of the Nigeria Data Protection Act 2023

²⁸⁹ O Babalola, 'Nigeria's Data Protection Legal and Institutional Model' (2022) 12(1) *International Data Privacy Law* 44.

²⁹⁰ O J Gstrein and A J Zwitter, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?'

The judiciary is another important organ in enforcement. Courts interpret privacy provisions, adjudicate disputes, and grant remedies to aggrieved parties. Through judicial interpretation, the courts contribute to the development of data privacy jurisprudence and clarification of legal principles governing the processing of personal data.

Another main actor is the law enforcement agencies. Under the Cybercrimes Act, organizations such as the Economic and Financial Crimes Commission (EFCC) and the Nigerian Police are to investigate offences relating to data breaches.²⁹¹ Their participation, however, is particularly relevant where data privacy violations constitute criminal offences.

Institutional enforcement is also extended to private actors. Data controllers and data processors take the direct responsibility for compliance and many need to designate Data Protection Officers. Industry associations and professional bodies can supplement official enforcement by encouraging self-regulation and standards of compliance. Professional associations, industries, and civil society organizations also contribute to the enforcement ecosystem by promoting awareness, encouraging compliance, developing best practice standards, and supporting advocacy initiatives aimed at strengthening data protection culture within society.²⁹²

Additionally, Nigeria's enforcement agencies should work with global regulators, join regional initiatives, and establish cooperation agreements due to the cross-border

(2021) 10 *Internet Policy Review*.

²⁹¹ Ifeoma Nwafor, 'Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps' (2025) *African Journal of Legal Studies* 260–261.

²⁹² F A Nwodo and C O Amucheazi, 'Analysis of Regulatory Strategies to Ensure the Independence of Nigeria's

Data Protection Commission' (2025) 15(1) *International Data Privacy Law*.



nature of digital data.²⁹³ Without this, enforcement is going to stay nationally isolated in a globally connected cyber space. As a guiding maxim reminds policy makers: "No law can be stronger than the institutions through which it lives." Nigeria's problem then is not only to legislate, but to build strong, capable, and independent institutions that can effectively implement the data privacy law.

CHAPTER FOUR

²⁹³ Section 5 and section 6 of Nigeria Data Protection Act 2023.



CHALLENGES AND PROSPECTS OF ENFORCING DATA PRIVACY IN NIGERIA

4.1 Challenges of Enforcing Data Privacy

4.1.1 Weaknesses of Institutions and Regulation

Institutional limitations are a major part of the weakness of data privacy in Nigeria. The Nigeria Data Protection Commission (NDPC) is still relatively young. They are not yet institutionally mature, not financially independent and not staffed at levels necessary to enforce compliance in a complex digital environment.²⁹⁴ Without strong infrastructure, the NDPC would be another regulatory body with limited resources in an already fragmented institutional governance environment.²⁹⁵ A particular shortcoming is in competing competencies. Although the NDPC is now the principal data protection authority in Nigeria, sector-specific regulators such as the Nigerian Communications Commission, the Central Bank of Nigeria and NITDA continue to have roles that overlap into privacy. “This overlap leads to confusion, duplication, and at times diverging guidance to regulated entities.”²⁹⁶

Another institution weakness is that awareness of rights is absent in the public.²⁹⁷ The strongest legal regime cannot help if citizens do not know their rights or how to enforce them. Most Nigerians are not aware of how to file complaints to the NDPC or seek

²⁹⁴ O Babalola, ‘Nigeria’s Data Protection Legal and Institutional Model’ (2022) 12(1) *International Data Privacy Law* 44.

²⁹⁵ Sumayya Babangida Sabo and Samuel Avemaria Utulu, ‘Organization Studies Based Appraisal of Institutional Propositions in the Nigeria Data Protection Regulation’ in Proceedings of the Cyber Secure Nigeria Conference (Nigerian Army Resource Centre, Abuja, 11–12 July 2023) 115.

²⁹⁶ Patrick Chukwunonso Aloamaka, ‘Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions’ (2023) 3(1) *UCC Law Journal* 281.

²⁹⁷ Patrick Chukwunonso Aloamaka, ‘Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions’ (2023) 3(1) *UCC Law Journal* 281.



remedies in the court.²⁹⁸ Without ongoing public education, the system is at risk of being used only by the few who are legally literate, or who are affiliated with groups doing advocacy.²⁹⁹ Institutional coordination is also absent, which makes enforcement difficult. Protecting data privacy through regulatory and law enforcement cooperation and even involving private actors is essential. However, most Nigerian institutions work in silos and have little collaboration and information sharing. This lack of synergism destroys efficiency.³⁰⁰ There is also the problem of institutional capture. The regulatory agencies in Nigeria have not been able to remain independent without political and commercial influence. If the NDPC succumb to similar pressures, the powerful data controllers will be able to avoid accountability which could weaken compliance and enforcement credibility.

The most basic institutional flaw is its funding.³⁰¹ Without adequate budgetary allocation, enforcement will be restricted to issuing guidelines instead of audits, inspections and prosecutions.³⁰² The lack of funds also limits the NDPC's capacity to participate in public awareness, international cooperation or technology tracking. As one analyst has rightly observed: "Institutions are the blood of enforcement; without well resourced, independent and empowered institutions, even the most progressive

²⁹⁸ F A Nwodo and C O Amucheazi, 'Analysis of Regulatory Strategies to Ensure the Independence of Nigeria's

Data Protection Commission' (2025) 15(1) *International Data Privacy Law* 67.

²⁹⁹ A I Uwadinma, 'Data Privacy and Consumer Protection in Nigeria's Digital Economy: A Legal Examination of

the Nigeria Data Protection Act, 2023' (2025) 1(1) *AUN Journal of Law* 25.

³⁰⁰ S O Akintola, 'Nigerian Data Protection Regulation 2019: A Critical Appraisal' (2021) 11(3) *International Data*

Privacy Law 307.

³⁰¹ Olumide Babalola, *Nigeria Data Protection Act 2023: A Commentary* (Olumide Babalola LP 2023) 45.

³⁰² Ayodele Akenroye, 'Nigeria's Data Protection Act 2023: Enforcement Challenges' (2023) *African Journal of*

Law and Technology 12(2) 33.



legislation remains nothing more than ink on paper.³⁰³ This summarizes Nigeria's institutional conundrum in enforcing data privacy.

4.1.2 Constraints on Technologies and Infrastructure.

Data privacy enforcement does not happen in a vacuum; its enforcement is closely linked to technological and infrastructural capability. In this regard, Nigeria has substantial constraints. Unlike the developed world jurisdictions with the ability to monitor, trace and punish complex digital offences, Nigeria lacks the technological infrastructure to identify, trace and punish complex digital offences.³⁰⁴

One of the immediate problems is the lack of central monitoring infrastructures. Advanced economy regulators are increasingly using real-time technologies for compliance monitoring, breach detection and cross-border tracing. In Nigeria, enforcement is still predominantly manual, report and complaint-based, a reactive and not a preventive approach. Cyber security infrastructure, however, remains fragile. Many government databases are not encrypted, lack intrusion detection, and don't incorporate secure cloud protocols.³⁰⁵ These vulnerabilities leave sensitive citizen information at risk of breaches which not only leads to a loss of faith in the government but also makes enforcement more complex. If the state itself does not have secure systems, then a law cannot protect data. Technological enforcement also needs a stable internet infrastructure and stable electricity supply. Continuous challenges in the areas of electricity and broadband access in Nigeria restrict the ability of regulators and

³⁰³ D D Oyawole, 'An Assessment of the Scope and Enforcement of Data Subject Rights under Nigerian Data

Protection Regimes' (2023) *Lawrit Journal of Law* Vol V Issue II 40.

³⁰⁴ A Omotubora, 'Privacy by Design and the eNaira: Ensuring Data Protection in Nigeria's Central Bank Digital

Currency' (2024) 68(2) *Journal of African Law*.

³⁰⁵ Ibid



organisations to support compliance mechanisms. Rural communities are less well-affected than urban areas. Many citizens are unserved by technological infrastructure, and are therefore outside the scope of privacy protection. Technology is changing so quickly it makes this even more complicated.³⁰⁶ Innovative technologies such as artificial intelligence, biometrics and big-data data analytics present new privacy challenges that are beyond the scope of Nigerian regulators' current tools. By the time the institutional response is developed, the technology has often developed further, producing a continuous lag effect in enforcement. There is also poor cross-sectoral integration. Technological systems within government agencies need to be connected to each other in a secure way to enforce data privacy. In Nigeria, interoperability of systems and databases is a key problem that hinders such coordination, increasing the likelihood of breaches and increasing the difficulty of enforcement³⁰⁷

Another shortcoming is that there is little local innovation in terms of compliance technology applications. Many organizations rely on foreign data protection software which is expensive and sometimes not compatible with the Nigerian regulatory environment. Without domestic ability to develop compliance technologies, enforcement will continue to be externally dependent.³⁰⁸ An additional issue is that of digital forensics capacity. In order to investigate breaches, it is essential to have advanced forensic tools and trained personnel with the expertise to analyze digital

³⁰⁶ J O Effoduh, 'Toward a Trustworthy and Inclusive Data Governance Policy for the Use of Artificial Intelligence

in Africa' (2024) 6 *Data & Policy* e34.

³⁰⁷ M Amutorine, S Wamala and P Kyeyune, 'Increasing Data Sharing and Use for Social Good: Lessons from

Africa's Data-Sharing Practices During the COVID-19 Response' (2024) 6 *Data & Policy* e29.

³⁰⁸ S Singler and O Babalola, 'Digital Colonialism Beyond Surveillance Capitalism? Coloniality of Knowledge in

Nigeria's Emerging Privacy Rights Legislation and Border Surveillance Practices' (2025) 34(5) *Information &*

Communications Technology Law 487.



evidence.³⁰⁹ Data crimes are still weak in terms of prosecutions because Nigerian law enforcement agencies are still building the capacity to investigate and prosecute these offences.³¹⁰ Nigeria's infrastructural and technological limitations pose a significant challenge to the effective implementation of data privacy policies.³¹¹

4.1.3 Jurisdictional and Cross-Border Data Issues

The digital age is by its very nature transnational. Data crosses borders easily, and what's done in one jurisdiction is often defeated by what's done in another. One challenge that Nigeria is faced with data privacy enforcement is jurisdictional and cross-border challenges. The problem includes the absence of effective control over cross-border transfers.³¹² Nigerian regulators have no easy way of tracing how companies transfer data into servers in Europe, America or Asia. Another related problem is the extraterritorial enforcement gap.³¹³ A number of multinational companies that process data collected on Nigerian citizens are incorporated and primarily regulated outside Nigeria examples META platforms, Google LLC, Microsoft Corporations. Therefore, the effective regulation of these entities requires international cooperation and Nigeria has failed to institutionalize properly.³¹⁴ Another difficulty is the conflicts of laws that arises in cross border data transfer. Data protection regulations are different from one

³⁰⁹ Ifeoma Nwafor, 'Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps' (2024) 16(3) *African*

Journal of Legal Studies 249.

³¹⁰ *Ibid* 260

³¹¹ Chidiebere Johnson Odo, 'Limitations of Digital Forensic Investigation in Nigeria's Rural Communities' (2025)

Emerging Minds Journal for Student Research.

³¹² T Ilori, 'Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2023) 23(2) *African Human Rights*

Law Journal 899.

³¹³ Cross-Border Data Transfers Under Nigeria's NDPA: A Compliance Guide' (Mondaq, 29 May 2026)

<https://www.mondaq.com/nigeria/privacy-protection/1793876/cross-border-data-transfers-under-nigerias-ndpa-a-compliance-guide>.

last accessed 6 June 2026.

³¹⁴ Nigeria Data Protection Act 2023, s 42(2)(b)

jurisdiction to the next that is the issue of dual criminality.³¹⁵ For instance, the GDPR is a regime that has strict safeguards, whereas other jurisdictions might have looser regimes. International businesses of Nigerian origin can be challenged on the basis of competing compliance standards, and regulators may have difficulty claiming jurisdiction over overseas actors.³¹⁶

In addition, Nigeria has no regional enforcement bodies within the African region. Although the African Union has adopted the Malabo Convention on Cybersecurity and Data Protection, ratification and implementation have been slow. The lack of regional cooperation results in Nigeria being alone in efforts to take cognizance of privacy breaches across borders.³¹⁷

4.1.4 Attitudes towards privacy in cultures and society.

How data privacy laws are enforced in Nigeria are heavily influenced by cultural and societal notions of privacy. Unlike western societies whose view of privacy is framed around the rights of individuals, Nigerian society is traditionally oriented towards the values of communal values and collective identity. As a result of the low awareness of privacy rights, it is not immediately obvious to the individual that the misuse of his or her information is a serious violation. The absence of a privacy conscious culture hurts enforcement efforts.³¹⁸ In every general transaction, Nigerians give away personal

³¹⁵ W Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) *Washington International Law Journal* 485, 490–495.

³¹⁶ F A Nwodo, 'Nigeria's Data Protection Commission: Insulation, Independence, and Accountability under the NDPA 2023' (2025) 15(1) *International Data Privacy Law*.

³¹⁷ Graham Greenleaf, *Global Data Privacy Laws 2024: Despite Problems, 80% of the World Has Data Privacy Laws* (2024) 183 Privacy Laws & Business International Report 1.

³¹⁸ O Osho and A Adebisi, 'Data Protection and Privacy Awareness in Nigeria: Challenges and Prospects' (2021)

5(2) *Nigerian Journal of Technology* 215.



sensitive information like phone numbers, addresses or bank information without asking why or how the information will be utilized.³¹⁹ Therefore, this attitude towards personal data sets the stage for private and public institutions to exploit information without significant opposition. In addition, the individuals are discouraged because they lack confidence in public institutions, as a consequence, even when people know that their data rights have been breached, they may not seek to enforce their rights, thinking that complaints will be dismissed or poorly resolved. This weakens the deterrence function of data protection laws.³²⁰

Regulator awareness campaigns have been few and largely urban in nature.³²¹ In rural areas where digital literacy is often low, the concept of data privacy is a foreign one.³²² Enforcement is then confronted with a double paradox: citizens do not demand accountability, and the violators take advantage of the ignorance. Without cultural awareness, legal reforms will continue to be disconnected from the population at large. Religious and cultural norms can also weaken the privacy discourse.³²³ In communities in which elders, leaders or institutions are accorded unquestioned access to personal information, raising issues about the privacy implications of such practice may be

³¹⁹ Tiwalade Adelola, Ray Dawson and Firat Batmaz, 'Nigerians' Perceptions of Personal Data Protection and Privacy' (SQM Conference 2015)

https://www.researchgate.net/publication/275968129_Nigerians%27_Perceptions_of_Personal_Data_Protection_and_Privacy. Last accessed 5 June 2026.

³²⁰ F A Nwodo, 'Nigeria's Data Protection Commission: Insulation, Independence, and Accountability under the NDPA 2023' (2025) 15(1) *International Data Privacy Law*.

³²¹ Centre for Information Technology and Development (CITAD), *Less than 20% of Nigerians Aware of Data Protection Law* (Daily Trust, 2025) <https://dailytrust.com/less-than-20-of-nigerians-aware-of-data-protection-law-citad/> accessed 6 June 2026 at 2:26pm.

³²² B Faturoti and I Juma, 'Enforcing data privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice' (2025) *International Review of Law, Computers & Technology* 1-25.

³²³ R Clarke, 'Privacy and Culture' (2014) *Computer Law & Security Review* 30(5) 569–586.



considered culturally inappropriate or even disruptive.³²⁴ Thus, the social institutions themselves can limit the enforcement of privacy rights.

Economic pressures further undermine people's commitment to privacy. For example, the financially challenged in Nigeria, to them concern for privacy may seem important for their survival. People will willingly exchange personal information for relatively minimal benefits like free Internet access, financial rewards, access to social programs, without realizing the long-term consequences of such transactions.³²⁵ These attitudes are regularly taken advantage of by the private sector like Telecommunications firms, marketers and financial institutions. This acceptance of exploitation allows for weak enforcement to continue. Unlike other human rights concerns in Nigeria, such as freedom of expression or anti-corruption, little public level campaigning exists around privacy. Laws are most effective when they reflect public values therefore where privacy is not widely seen as an important right, enforcement will be weak.³²⁶

4.1.5 Uncertainty in Judicial Application and Remedies

Judicial interpretation is an important role in the implementation of data privacy rights but Nigeria's courts have not developed consistent rules in this regard. This unpredictability deprives legal remedies of much of their predictability, dissuades people from seeking redress, and reduces the deterrent effect of the law.³²⁷ The

³²⁴ I E Nwafor, 'Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps' (2024) 16(3) *African Journal of Legal Studies* 249.

³²⁵ Ibrahim Al-Jabri, 'The Willingness to Disclose Personal Information: Trade-off between Privacy Concerns and Benefits' (2020) 28 *Information & Computer Security* 161.

³²⁶ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

³²⁷ Jan Broulík, 'Predictability: A Mistreated Virtue of Competition Law' (2024) 12(3) *Journal of Antitrust Enforcement* 362, 363–365



constitutional grounding of privacy rights stated in Section 37 of the Constitution of 1999 provides for the privacy of citizen, homes, correspondence and telephone conversations. However, courts have been hesitant to stretch this provision to expressly include digital data, the narrow interpretation results in gaps of protection. In *Ransome-Kuti v Attorney-General of the Federation*³²⁸, the Court emphasized that fundamental rights must be interpreted strictly within the wording of the Constitution. Different courts have used different criteria in determining whether there is a privacy violation. While some courts must establish actual harm (such as a financial loss) before awarding remedies, other courts have held that mere breach of data confidentiality is enough to be considered harm. In *Emerging Markets Telecommunication Services Ltd v Eneye*³²⁹, where the Supreme Court recognized the legal effect of the unauthorized handling and disclosure of subscriber information. The case shows that organizations that collect personal data have a duty to protect it, and that privacy breaches can lead to legal remedies even where no financial loss is proved. This inconsistency confuses litigants and waters down the force of privacy enforcement. Many judges are not trained for complex data protection cases or digital forensics or cyber law due to the emerging technologies. As a result, they also sometimes fall back to outdated analogies of the legal world to interpret complex digital privacy dispute.³³⁰ Further, delays in the judicial process frustrate enforcement. Privacy breaches often demand quick remedies, injunctions to stop continued misuse of data.³³¹ However, with Nigeria's backlog of cases in the judicial system, it can take years for cases to be resolved, at which point

³²⁸ (1985) 2 NWLR (Pt 6) 211 (SC).

³²⁹ 2018) LPELR-43706(SC).

³³⁰ Chukwuebuka Usulor, 'Specialist and Problem-Solving Courts: The New Paradigm for Justice Administration in Nigeria' (2024) *NAU Law Review* 3(2).

³³¹ C J Ubanyionwu, 'Solving the Problem of Delay in Adjudication of Cases in Nigeria through Artificial Intelligence (AI)' (2025) 2(1) *Journal of Customary and Religious Law* 136–148.

the harm may have become permanent. This is detrimental to the effect of remedies of the judiciary. Inconsistency arises from the absence of clear guidance from appellate courts. Only a few privacy-related cases have gone to the Court of Appeal or Supreme Court and thus the number of binding precedents available has made some areas of the law without judicial guidance.³³² Another shortcoming is the absence of alignment between judicial remedies and regulatory sanctions. While the NDPC may issue fines or compliance orders, courts can issue conflicting rulings, resulting in ambiguity for regulated entities.³³³ Judicial independence should also be included especially in politically sensitive cases such as those relating to surveillance, or government access to private data, the courts are less likely to examine state bodies. Such selective enforcement damages public trust in the courts' ability to protect privacy rights.³³⁴

4.6 Prospects for Effective Enforcement

Despite the significant challenges analyzed above, Nigeria's data privacy enforcement landscape is not without promise. Several enabling factors and emerging opportunities present a realistic pathway toward more effective protection of personal data rights in the digital age. These prospects operate at the institutional, technological, social, and international levels, and together suggest that meaningful improvement is achievable if deliberate and coordinated action is taken.

4.2.1 Strengthening Legal Institutions

The establishment of the Nigeria Data Protection Commission (NDPC) under the NDPA

³³² O V C Okene and O M Dimgba, 'Delay in the Administration of Justice in Nigeria: Causes and Remedies' (2022) 13(2) *Nigerian Juridical Review* 145, 148–151.

³³³ Fola Adeleke, 'Reinstating trust in elections in the era of artificial intelligence and emerging technologies' (2025)

7 *Data & Policy* e38 <https://doi.org/10.1017/dap.2025.14>.

³³⁴ Abdul Yusuf and Ajibolu Afolabi, 'The Judiciary and the Rule of Law' (2023) 8(1) *Journal of International Law and Jurisprudence* 1–20.



2023 represents a significant institutional step forward. Before the NDPA was enacted data protection was regulated through the NDPR 2019, which was enforced by the national information technology development agency (NITDA). However, the NITDA was responsible for several aspects of information technology regulation and was not created solely to oversee data protection. As a result, privacy regulation did not receive the same level of specialized attention that a dedicated authority could provide.³³⁵ The NDPC provides a centralized, dedicated authority empowered to receive complaints, conduct investigations, carry out audits, and impose sanctions.³³⁶ Strengthening the NDPC's independence, funding, and technical workforce must be a legislative and executive priority. As the agency responsible for the regulation of data protection, the commission needs adequate funding and skilled professionals to discharge their duties like investigations, monitor compliance and respond to complaints from the public.³³⁷ Additionally, the judiciary must be equipped with the capacity to adjudicate digital privacy disputes, through specialized training for judges in data protection law, digital forensics, and cyber-related evidence. Without judicial competence, enforcement will remain incomplete regardless of regulatory action.³³⁸

4.6.2 Enhancing Public Awareness and Digital Literacy

For data privacy laws to be effective, people must first be aware of the rights available to them. Most Nigerians are unaware of their data rights, which reduces the volume of complaints reaching the NDPC, demanding accountability or pushing the government to

³³⁵ Fochi Amabilis Nwodo and Chibike Oraeto Amucheazi, 'Analysis of Regulatory Strategies to Ensure the Independence of Nigeria's Data Protection Commission' (2025) 15(1) *International Data Privacy Law* 91.

³³⁶ Nigeria Data Protection Act 2023, section 5–6

³³⁷ Bukola Faturoti and Isaac Juma, 'Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice' (2025) *International Review of Law, Computers & Technology* 1, 10–16.

³³⁸ Chukwuebuka Usulor, 'Specialist and Problem-Solving Courts: The New Paradigm for Justice Administration in Nigeria' (2024) 3(2) *Nnamdi Azikiwe University Law Review* 19.

take stronger action. Through deliberate public education campaigns, school programs, targeting both urban and rural populations, citizens can gain basic understanding of the importance of protecting personal information. This is a strong foundation for enforcement, because informed citizens are more likely to demand accountability and supports the efforts of the regulators.³³⁹

4.6.3 Leveraging Technology for Data Protection

Technology, while presenting challenges to data privacy, also offers tools that can strengthen enforcement. Tools such as encryption, automated compliance system, data breach detection software, and digital forensic technologies.” Cavoukian’s foundational work on privacy-by-design demonstrates that embedding data protection principles into systems architecture from the outset is far more effective than reactive enforcement after breaches occur. Nigeria should invest in building domestic technological capacity and tools to ensure compliance is monitored. These technologies offer an opportunity to strengthen data privacy and the reduce the breaches involved.³⁴⁰

4.6.4 Regional and International Cooperation

Given the transnational nature of digital data flows that is data easily cross borders, no nation can enforce data privacy effectively on its own. Therefore, Nigeria’s ability to enforce data privacy effectively depends on the cooperation with other countries and regional bodies. This includes that the NDPC should actively enter into bilateral and multilateral data-sharing agreements work with international privacy networks such as

³³⁹ Dede Ibiere Peter and Ben-Collins Emeka Ndinojuo, ‘Privacy Awareness and Social Media: Personal Data Protection among Facebook and Instagram Users’ (2024) 6(3) *Galactica Media: Journal of Media Studies* 168, 180–185.

³⁴⁰ Chibuzo Okonkwo, ‘Data Protection and Cybersecurity Regulation in Nigeria: Challenges and Prospects’ (2023) 4(2) *Nigerian Journal of Technology Law* 55–72.

Global Privacy Assembly and Global Privacy Enforcement Networks³⁴¹, also take a leadership role in African Union data protection initiatives, including the domestication of the Malabo Convention. Within ECOWAS, Nigeria is well placed to champion the harmonization of regional data protection standards this would enable the regulation of the multinational companies on data protection. African approach to regulatory practice should be developed to the extent that it acknowledges Africa's institutional realities while conforming with global frameworks like the GDPR.³⁴² Such cooperation would not only strengthen Nigeria's enforcement reach against multinational actors but would signal Nigeria's commitment to digital rights as a pillar of its broader governance agenda.

³⁴¹ Global Privacy Assembly, *About the GPA* <https://globalprivacyassembly.org/about/>
Global Privacy Enforcement Network, *About GPEN* <https://www.privacyenforcement.net/content/home-public>.

(International networks of data protection authorities that promotes cooperation, information sharing, and

cross-border enforcement of privacy laws).last accessed 7 June 2026

³⁴² Emmanuel Salami, 'Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection

Law in Africa' (2022) 66(2) *Journal of African Law* 281–291.



CHAPTER FIVE

SUMMARY OF FINDINGS, RECOMMENDATIONS, AND CONCLUSION

5.1 Summary of Findings

This study has investigated the enforcement of data privacy law in Nigeria in the digital age, the challenges and prospects facing the regulatory framework in Nigeria as mainly set by the Nigeria Data Protection Act (NDPA) 2023. The study was geared towards doctrinal methodology that involved statutory interpretation, judicial rulings, regulators' instruments, and the academic literature to examine the effectiveness and sufficiency of Nigeria's data protection regime.

The study identified Nigeria's progress in the data protection laws, first, as a meaningful progress. NDPA 2023 has shifted the country on a more coordinated system to a better defined system and a more central authority. The NDPC now has powers to audit, investigate complaints and impose sanctions, making a significant enhancement in data protection governance. The fact that the Act mirrors the international standards, in particular the EU's GDPR and South Africa's POPIA, further signals Nigeria's commitment to meaningfully engage with international data governance norms.

Second, however, the researchers discovered that the enforcement is the least robust aspect of the Nigerian data privacy regime. The institutional shortcomings, such as the evolving capacity of the NDPC, insufficient resources and potential political manipulation, hinder the NDPA in practical implementation. The technological and infrastructural hurdles also make it difficult to enforce, with regulators facing a lack of means to monitor the complex digital landscape, investigate breaches committed by foreign actors and detect cross-border data flows. Secondly, there has not been a consistent development of privacy jurisprudence in the judiciary, and litigants are left



with disparate remedies, and no clear deterrence for data controllers in violation of the privacy laws.

Third, there are socio-cultural attitudes toward privacy, low digital literacy and lack of public awareness of data rights that mitigate enforcement. If citizens are not aware of their rights and what to do when they are infringed, then the enforcement is not backed by citizen participation but rather on the goodwill of regulators and government actions. Last, however, is the failure to regulate the data processors who are multinational and outside Nigeria which presents a huge loophole that can only be addressed by the national legislation.

5.2 Recommendations

1. A critical suggestion from this study is that the NDPC must be strengthened, not only separated from the law, but also be well funded, and technical skills must be provided. This would put enforcement capacity on par with the best data protection authorities in the world.
2. Harmonization of Data Protection Regulations in Nigeria is needed. This can be achieved by making sure that the roles of these regulators are clearly defined and differentiated each from the other so that they do not overlap and or cause confusion. This would establish legal divides and facilitate a more efficient and effective enforcement process.
3. National assembly should review and enact tougher punishment policies. Existing Fines are typically not large enough to deter powerful corporations that violate data rights. Penalties should be commensurate with ability of the organization; penalties should be more severe for larger company. Remedies



available those affected should be strengthened to ensure adequate compensation and protection of their rights.

4. Technological infrastructure needs to be better. Regulators need to foster sophisticated systems of monitoring compliance, detecting breaches and forensic investigations. Enforcement will continue to be reactive and ineffective when it is without the help of modern technological aids.
5. Public awareness campaigns need to be enlarged. There is a need to educate citizens about the importance of data privacy, the risks and possible solutions under the law. This can be achieved through public sensitization programmes and digital illiteracy initiatives. Ultimately, the culture of data rights will develop through pressure from a privacy conscious society on institutions.
6. Nigeria should pursue cooperation in data regulations with other countries. Data transfer and privacy mechanisms will strengthen Nigeria's capacity to hold foreign corporations accountable for violations of its citizens' rights under bilateral treaties, by sharing the same rights with international multilateral frameworks, and by duplicate rights.
7. Ensure civil society organizations, digital rights advocacy groups, public interest organizations, have a watchdog function on data protection. Citizen Advocacy groups can serve as a link between the people and regulators, educate the public, start strategic litigation, and monitor corporate activity.
8. Finally digital literacy should be mainstreamed into Nigeria's education system. Data privacy and privacy rights of individuals should be embedded at all levels to create the long-term cultural appreciation of privacy rights within the society as a



whole.

5.3 Conclusion

Nigeria is at a pivotal point in its quest for data privacy. The NDPA 2023 is a step forward in this respect, as for the first time it provides data privacy protection with the force of legislation, with its own enforcement commission and with a mechanism outlining rights and obligations largely in line with international best practice. The effectiveness of the legislation will depend on the strength of the institutions, resources and awareness to support it in practice.

The law-enforcement challenge between the formal and the factual situation in Nigeria is huge but not insurmountable, as this study has shown. All the challenges, institutional shortcomings, technological deficits, cultural apathy, judicial conservatism and the jurisdictional fragmentation are significant, but nothing new. While the EU and South Africa experiences cannot be directly imported, they can be used as valuable lessons. It is not just about legislative changes, it's about a new form of government and stakeholders thinking that data privacy is a constitutional value, not a compliance item on a checklist.

With its population over 142 million now using the internet, and the use of fintech, e-commerce and AI increasingly changing the way the people of Nigeria live, the safeguarding of their personal information is a democratic concern, not a technical one. The dignity, freedom and trust of a person rely on the attitude of the state with regard to the enforcement of their data rights.

The study, therefore, ends by concluding that robust internal institutions, resource availability, citizens' awareness, a capable judiciary and international collaboration are

all necessary but they must be aligned towards a genuine political will to focus on the rights of the individual in Nigeria's digital governance framework in order to enforce data privacy effectively. There is a convergence that is attainable. Now what's left is the combined effort to make it happen.



BIBLIOGRAPHY

BOOKS

Akenroye A, *Nigeria's Data Protection Act 2023: Enforcement Challenges* (2023)

Babalola O, *Data Protection Compliance in Nigeria* (Snap Press 2020)

Babalola O, *Data Protection Law and Practice in Nigeria* (Law Lords 2020)

Babalola O, *Nigeria Data Protection Act 2023: A Commentary* (Olumide Babalola LP 2023)

Beccaria C, *On Crimes and Punishments* (Henry Paolucci tr, originally published 1764, 1963 edn)

Becker GS, *The Economic Approach to Human Behavior* (University of Chicago Press 1968)

Bennett CJ and Raab CD, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006)

Bentham J, *The Panopticon Writings* (Miran Božovič ed, Verso 1995)

Birnhack M, *Constitutional Privacy and Data Protection in Comparative Perspective: Lessons from South Africa* (2021)

Bottoms A and von Hirsch A, 'The Crime-Preventive Impact of Penal Sanctions' in Anthony Bottoms and Andrew von Hirsch (eds), *The Oxford Handbook of Criminology* (4th edn, OUP 2012)

Burri M (ed), 'Safeguarding Privacy and Other Users' Rights in the Age of Big Data' in *Big Data and Global Trade Law* (CUP 2021)

Bygrave LA, *Data Privacy Law: An International Perspective* (OUP 2014)

Cate F, *The Failure of Fair Information Practice Principles in Consumer Protection in the Age of the Information Economy* (Ashgate 2006)

Clarke RV and Cornish DB, 'Modeling Offenders' Decisions: A Framework for Research and Policy' in Michael Tonry (ed), *Crime and Justice: An Annual Review of Research* (vol 6, University of Chicago Press 1985)

Cohen JE, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019)

Cohen JE, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012)



Dicey AV, *Introduction to the Study of the Law of the Constitution* (10th edn, Macmillan 1959)

Floridi L, *The Ethics of Information* (OUP 2013)

Foucault M, *Discipline and Punish: The Birth of the Prison* (Vintage Books 1975)

Greenleaf G, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP 2014)

Kitchin R, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Sage 2014)

Kuner C, *Transborder Data Flows and Data Privacy Law* (OUP 2013)

Kuner C, Bygrave LA and Docksey C, *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2024)

Lyon D, *Surveillance Studies: An Overview* (Polity Press 2007)

Lynskey O, *The Foundations of EU Data Protection Law* (OUP 2015)

Nissenbaum H, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010)

North D, *Institutions, Institutional Change and Economic Performance* (CUP 1990)

Nwabueze BO, *Constitutional Democracy in Africa* (Spectrum Books 2003)

Solove DJ, *Understanding Privacy* (Harvard University Press 2008)

Solove DJ and Schwartz PM, *Information Privacy Law* (5th edn, Aspen Publishers 2021)

Svantesson DJB, *Private International Law and the Internet* (3rd edn, Kluwer Law International 2021)

Uwadinma AI, *Data Privacy and Consumer Protection in Nigeria's Digital Economy: A Legal Examination of the Nigeria Data Protection Act 2023* (University of Abuja Press 2025)

Westin AF, *Privacy and Freedom* (Atheneum 1967)

Yemi Akinseye-George, *Constitutional Law and the Rule of Law in Nigeria* (MIJ Professional Publishers 2012)

JOURNAL ARTICLES

Abdullahi IA, 'An Appraisal of the Institutional Framework under the Nigeria Data



Protection Act 2023' (2024) *Nigerian Journal of Public Law*

Adediran OA, 'Child Privacy and Digital Rights in Nigeria: Legal Obligations and Protections' (2023) 14 *African Journal of Law and Technology* 112

Adeboyejo O, 'Cybersecurity, Privacy and Legal Protection of Personal Data in Nigeria' (2020) 12 *African Journal of Law and Technology* 56

Adegbite OA, 'Data Protection and Cybersecurity Challenges in Nigerian Digital Banking' (2021) 15(2) *Journal of Banking and Financial Law* 45

Adegbite T, 'NDPR Compliance Challenges in Nigeria' (2021) 15 *Journal of ICT Law* 78

Adeyemi A, 'Sectoral Regulation of Data in Nigeria Before the NDPR' (2018) 8 *Nigerian Journal of Technology Law* 33

Adeyemi O, 'Data Privacy Awareness in Nigeria' (2022) 3 *Lagos Law Review* 56

Agaba E, 'Public Awareness and Data Protection in Nigeria' (2021) 19 *Nigerian Law and Policy Review* 74

Aimasiko AE, 'The Constitutionality of Fine Imposition Under the Nigeria Data Protection Act 2023 and its Implications' (2024) *International Journal for Public Policy, Law and Development*

Akinboade T and Salami D, 'Data Privacy and Enforcement in Nigeria: A Regulatory Perspective' (2022) 9(1) *African Journal of Law and Technology* 21

Akintayo AE, 'Trends and Implications of Nigerian Courts' Jurisprudence on Privacy and Data Protection: Lessons from Comparative Foreign Jurisprudence' (2024) 1 *African Journal on Privacy and Data Protection* 99–118

Akintola SO, 'Nigerian Data Protection Regulation 2019: A Critical Appraisal' (2021) 11(3) *International Data Privacy Law* 307

Al-Jabri I, 'The Willingness to Disclose Personal Information: Trade-off Between Privacy Concerns and Benefits' (2020) 28 *Information and Computer Security* 161

Aloamaka PC, 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms' (2025) 4(2) *UCC Law Journal* 242

Aloamaka PC, 'Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions' (2023) 3(1) *UCC Law Journal* 281–321

Amutorine M, Wamala S and Kyeyune P, 'Increasing Data Sharing and Use for Social Good: Lessons from Africa's Data-Sharing Practices During the COVID-19 Response' (2024) 6 *Data and Policy* e29



Anyaegbunam AA, 'Legal and Institutional Framework for Data Protection in Nigeria' (2020) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 87

Arowolo AO, 'Enforcing Data Protection Rights in Nigeria: Legal and Institutional Constraints' (2022) 9 *Journal of African Law and Policy* 64

Atoyebi B and Omotubora A, 'Data Protection Regulation and Enforcement in Nigeria' (2020) 4 *Nigerian Journal of Technology Law* 55

Ayeni AO, 'The Role of the African Commission in Enhancing Implementation Monitoring Through Dialogue and Documentation' (2024) 24(2) *African Human Rights Law Journal* 937–961

Babalola O, 'Data Protection in Nigeria: The Journey So Far and the Road Ahead' (2020) *Gravitas Review of Business and Property Law*

Babalola O, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2021) 12(1) *International Data Privacy Law*

Babalola O, 'The EU GDPR and Nigeria's NDPR: A Comparative Analysis' (2021) 4(4) *Journal of Data Protection and Privacy* 372

Babalola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) *British Journal of Cyber Criminology*

Babalola O, 'Transborder Flow of Personal Data in Africa' (2024) 52 *Computer Law and Security Review*

Broulík J, 'Predictability: A Mistreated Virtue of Competition Law' (2024) 12(3) *Journal of Antitrust Enforcement* 362

Chukwumerije A, 'Privacy versus Security: Cybercrime Laws in Nigeria' (2021) 9 *African Journal of International and Comparative Law* 77

Clarke R, 'Definitions of Data in Information Governance' (2019) 14 *Journal of Information Privacy and Security* 33

Clarke R, 'Privacy and Culture' (2014) 30(5) *Computer Law and Security Review* 569–586

Cohen JE, 'What Privacy Is For' (2013) *Harvard Law Review*

De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law and Security Review* 179

Edgcumbe A, Currie J and McLennan S, 'Potato Potato? Disentangling De-Identification, Anonymization and Pseudonymization in Data Protection Law' (2025) 12(1) *Journal of*

Effoduh JO, 'Toward a Trustworthy and Inclusive Data Governance Policy for the Use of Artificial Intelligence in Africa' (2024) 6 *Data and Policy* e34

Eseyin M and Archibong S, 'An Examination of Surveillance Capitalism and the Erosion of Data Privacy in the Digital Economy in Nigeria' (2025) *Uniuyo Law Journal*

Faturoti B and Juma I, 'Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice' (2025) *International Review of Law, Computers and Technology* 1–25

Fried C, 'Privacy' (1970) 77 *Yale Law Journal* 475

Genevieve OC, 'Confidentiality and Public Health: An Examination of Legal and Ethical Frameworks Governing Doctors' Duty to Disclose Serious Health Conditions in Nigeria' (2025) *FUNAI Law Review Projects*

Greenleaf GW, 'International and Regional Commitments in African Data Privacy Laws' (2022) 46 *Computer Law and Security Review* 105743

Greenleaf G, 'Global Data Privacy Laws 2021: Current Status and Prospects' (2021) *Computer Law and Security Review* 101673

Greenleaf G, 'Global Data Privacy Laws 2024: Despite Problems, 80% of the World Has Data Privacy Laws' (2024) 183 *Privacy Laws and Business International Report* 1

Ilori T, 'A Postcolonial Legal Critique of the Appropriation of Online Expression in Africa' (2024) 68(1) *Journal of African Law*

Ilori T, 'Protecting Digital Rights Through Soft Law: Ensuring the Implementation of the Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2023) 23(2) *African Human Rights Law Journal* 899–923

Makulilo AB, 'Data Protection in Africa: A Comparative Perspective' (2016) *African Journal of Information and Communication*

Mohammed RO, Musa A and Ismail ZO, 'Big Data Adoption and E-Government Implementation in Nigeria' (2022) 12 *ATBU Journal of Science, Technology and Environmental Education*

Monye FN, Nwafor N and Mukoro B, 'Appraisal of the Nigerian Credit Reporting Act 2017' (2020) 64(2) *Journal of African Law* 229

Ncube H, 'Data Protection in Africa: A Comparative Perspective on the Protection of Personal Information Act' (2021) *African Human Rights Law Journal*

Nwafor I, 'Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps' (2024)

16(3) *African Journal of Legal Studies* 249

Nwankwo C, 'Digital Rights and Data Protection in Nigeria' (2020) *Journal of African Law and Technology*

Nwodo FA and Amucheazi CO, 'Analysis of Regulatory Strategies to Ensure the Independence of Nigeria's Data Protection Commission' (2025) 15(1) *International Data Privacy Law*

Obioha F, 'Harmonising Data Protection Laws in Nigeria: Challenges and Prospects' (2024) 11 *Journal of African Legal Studies* 67

Odo CJ, 'Limitations of Digital Forensic Investigation in Nigeria's Rural Communities' (2025) *Emerging Minds Journal for Student Research*

Ogban-Iyam JA, 'Privacy and the Dynamics of Social Control in Modern Nigeria' (2014) *Nigerian Journal of Social Sciences*

Okafor C, 'Assessing Nigeria's Data Protection Regime Post-NDPA 2023' (2024) *African Journal of Law and Technology*

Okonkwo C, 'Data Protection and Cybersecurity Regulation in Nigeria: Challenges and Prospects' (2023) 4(2) *Nigerian Journal of Technology Law* 55–72

Okonkwo FN, 'Children's Privacy and Data Protection in Nigeria: Legal and Institutional Responsibilities' (2022) 8 *Nigerian Journal of Law and Technology* 101

Olatunbosun OA, 'Digital Governance and Regulatory Challenges in Nigeria' (2021) 15 *Nigerian Journal of Public Law* 87

Omotubora A, 'Privacy by Design and the eNaira: Ensuring Data Protection in Nigeria's Central Bank Digital Currency' (2024) 68(2) *Journal of African Law*

Oraegbunam I and Iroanya EC, 'Section 12 of the 1999 Constitution of Nigeria and Treaty Implementation: A Legal Critique' (2023) 5(2) *International Review of Law and Jurisprudence*

Ottah OI and Imoisi ES, 'An Appraisal of the Legal Framework for Data Security Protection for Health Institutions in Nigeria' (2025) 16(2) *Journal of Current Research and Review*

Oyewole O, 'Re-thinking Privacy Rights in Nigeria's Digital Environment' (2019) *Nigerian Journal of Public Law*

Peter DI and Ndinojuo BCE, 'Privacy Awareness and Social Media: Personal Data Protection among Facebook and Instagram Users' (2024) 6(3) *Galactica Media: Journal of Media Studies* 168



Plantinga P and others, 'Responsible Artificial Intelligence in Africa: Towards Policy Learning' (2024) 6 *Data and Policy* e23

Sadiq UM, 'Personal Data Protection and Privacy in Nigeria's Emerging Digital Economy' (2020) 4 *African Journal of Law and Technology* 112

Salami E, 'Implementing the AfCFTA Agreement: A Case for the Harmonisation of Data Protection Law in Africa' (2022) 66(2) *Journal of African Law* 281–291

Salau AO, 'Cybersecurity, State Surveillance and the Right to Online Privacy in Nigeria: A Call for Synergy of Law and Policy' (2024) 1 *African Journal on Privacy and Data Protection* 152–161

Shehu I and Bello SR, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria' (2022) *Journal of Law, Policy and Globalization*

Singler S and Babalola O, 'Digital Colonialism Beyond Surveillance Capitalism? Coloniality of Knowledge in Nigeria's Emerging Privacy Rights Legislation and Border Surveillance Practices' (2025) 34(5) *Information and Communications Technology Law* 487

Thaldar D, 'The Protection of Personal Information Act and Constitutional Privacy in South Africa' (2020) *South African Journal on Human Rights* 341

Ugbo SN, Ajilore K and Ajaegbu O, 'Big Data Analytics Adoption in Brand Communication Campaigns: Evidence from Lagos State, Nigeria' (2021) *International Journal of Cambridge Research Publication*

Usulor C, 'Specialist and Problem-Solving Courts: The New Paradigm for Justice Administration in Nigeria' (2024) 3(2) *Nnamdi Azikiwe University Law Review*

Uwadinma AI, 'The Digital Economy and Consumer Protection in Nigeria: A Legal Analysis of Data Privacy Laws under the Nigeria Data Protection Act 2023' (2025) 1 *AUN Journal of Law*

van der Sloot B, 'Surveillance, Cybercrime and the Limits of Privacy' (2017) 3 *International Journal of Law and Information Technology* 101

Voss WG, 'Cross-Border Data Flows, the GDPR and Data Governance' (2020) 29(3) *Washington International Law Journal* 485–495

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193

Reports and Institutional Publications

African Union Commission, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)* (African Union 2014)



Centre for Information Technology and Development (CITAD), *Less than 20% of Nigerians Aware of Data Protection Law* (2025)

Central Bank of Nigeria, *Consumer Protection Framework* (CBN 2016)

Central Bank of Nigeria, *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers in Nigeria* (CBN 2018)

DataReportal (Kepios), *Digital 2024: Global Internet Use Accelerates* (DataReportal 2024)

Global Privacy Assembly, *About the Global Privacy Assembly*

Global Privacy Enforcement Network, *About GPEN*

GSMA, *The State of Mobile Internet Connectivity 2023* (GSMA 2023)

National Information Technology Development Agency, *Nigeria Data Protection Regulation 2019*

National Identity Management Commission, *Bank Verification Number Framework*

Nigeria Data Protection Commission, *Annual Data Protection Report* (NDPC 2024)

Nigeria Data Protection Commission, *International Journal of Data Privacy and Protection* (NDPC 2025)

Nigerian Communications Commission, *Subscriber Statistics Report* (January 2025)

Organisation for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2020* (OECD Publishing 2020)

Privacy International and Paradigm Initiative, *A State of Surveillance: Government Surveillance in Nigeria* (2018)

United Nations Conference on Trade and Development (UNCTAD), *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (UNCTAD 2016)

United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2021* (UNCTAD 2021)

United Nations Economic Commission for Africa, *Digital Transformation Strategy for Africa (2020–2030)* (UNECA 2020)

World Bank, *World Development Report 2021: Data for Better Lives* (World Bank 2021)

Conference Papers and Proceedings



Adelola T, Dawson R and Batmaz F, 'Nigerians' Perceptions of Personal Data Protection and Privacy' (SQM Conference 2015)

Ekpo O and Aiyetan O, 'A Comparative Analysis of Nigeria's NDPA and the EU's GDPR' in *Proceedings of the International Conference on Information Technology and Data Analytics* (ACM 2024)

Sabo SB and Utulu SA, 'Organisation Studies Based Appraisal of Institutional Propositions in the Nigeria Data Protection Regulation' in *Proceedings of the Cyber Secure Nigeria Conference* (Nigerian Army Resource Centre, Abuja, 11–12 July 2023)

Theses and Dissertations

Adewumi A, 'Adequate Protection: An Analysis of Nigeria's Data Protection Laws within an Emerging Framework' (LLM thesis, University of Victoria 2022)

Udofia K, *A Critical Analysis of Credit Information Sharing under Nigeria's Credit Reporting Act 2017* (SSRN Working Paper, 2017)

Newspapers

THISDAY Newspapers, 'Active Data Internet Subscribers Hit 142m as GSM Subscriptions Maintain Market Lead' (20 March 2025)

Daily Trust, 'Less than 20% of Nigerians Aware of Data Protection Law' (2025)

New Telegraph, 'NIN–SIM Linkage: Addressing Data Privacy Concerns' (2019)

Online Sources

Bank Verification Number, 'Bank Verification Number (BVN)' (Central Bank of Nigeria)

Cross-Border Data Transfers Under Nigeria's NDPA: A Compliance Guide (Mondaq, 29 May 2026)

Law Global Hub, 'Data Privacy or Data Exploitation? Testing Nigeria's Data Protection Act 2023'

Michalsons, 'AU Convention on Cyber Security and Personal Data Protection (Malabo Convention)' (updated 2023)

Nigeria Data Protection Commission, Official Publications

Oxford Learner's Dictionaries, 'Data'



