Fountain University Law Journal Vol. 3 No. 5, 2026

PRINT ISSN: 0794-0254

ONLINE: E-ISSN: 0794-084X

FRAGMENTED PROTECTIONS: INSTITUTIONAL BARRIERS TO CONSUMER DATA PROTECTION IN NIGERIA'S E-COMMERCE SECTOR

By

Oghomwen Rita Ohiro PhD*

Abstract

In Nigeria, there are persistent consumer data vulnerabilities in the e-commerce sector despite the enactment of several laws. This paper, through a doctrinal research methodology, analyzes relevant provisions of the Nigeria Data Protection Act (NDPA) 2023 and the Federal Competition and Consumer Protection Act (FCCPA) 2018. It engages in a comparative assessment of the European Union General Data Protection Regulation (GDPR) and the United States Federal Trade Commission (FTC) enforcement models, and a qualitative textual review of the privacy policies of two major Nigerian e-commerce platforms. The platform-policy review evaluates explicit disclosures regarding consent acquisition, retention periods, third-party data sharing, and withdrawal procedures against NDPA 2023 requirements. The study finds that legal issues originate primarily from overlapping regulatory mandates between the NDPC and FCCPC and weak enforcement rather than an absence of statutory provisions. Specifically, consent mechanisms fail to provide meaningful control because platforms use bundled terms, omit specified retention limits, and rely on regulatory provisions such as Article 17 (8)(b) of the General Application and Implementation Directive (GAID) 2025 that treat closing a notice pop-up as implied consent. To address these institutional gaps, the paper recommends establishing a binding joint NDPC-FCCPC enforcement framework, issuing sectoral e-commerce guidelines mandating symmetric "Reject All" choices, requiring user privacy dashboards, and enforcing specific data retention schedules.

Keywords: **Consumer Data, Privacy, Control, Consent, E-commerce, Consumer**

1.0 INTRODUCTION

Nigeria's e-commerce sector has experienced rapid growth driven by increasing internet penetration, smartphone adoption, and digital financial services.[1] Platforms such as Jumia, Konga, and PayPorte have become integral to the country's digital marketplace, offering consumers convenient access to goods and services.[2] E-commerce platforms collect vast amounts

* Senior Lecturer (Department of Public Law, Faculty of Law, University of Benin) Email: oghomwen.igbinedion@uniben.edu

[1] MuhammadSulaiman andFatima Isa, 'Assessing the Impact of Cybercrimeon the Growth and Sustainabilityof e-Commerce in Nigeria' *ABUAD Journal of Social and Management Sciences* (2025) 6(2) 272

[2] Ibid.

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

of consumer data including credit card information, personal profiles, employment details, and health fitness status during online transactions.[3]

The collection and processing of consumer data raise serious legal concerns, particularly where processing occurs without transparency, informed consent, or effective regulatory oversight.

It is important, however, to distinguish consent as merely one lawful basis for processing personal data from the wider array of obligations imposed by the Nigeria Data Protection Act (NDPA) 2023.[4] Section 25 of the NDPA recognises consent alongside other lawful bases, including performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest, and legitimate interests pursued by the data controller. Beyond establishing a lawful basis, the NDPA also imposes independent obligations on data controllers and processors, such as the principles of lawfulness, fairness, and transparency under Section 24, purpose limitation, data minimisation, accuracy, storage limitation, and accountability, as well as requirements relating to data protection impact assessments and breach notification. This means that even where consent is validly obtained, a controller's processing activities must still satisfy these broader statutory requirements, as consent alone does not exempt an organisation from complying with the Act's other obligations. Balancing data protection with the free flow of information, while preventing misuse by third parties, therefore remains a significant challenge. [5] Nigerian consumers are regularly required to disclose extensive personal and financial information to access online services, yet they often remain unaware of how this data is used, retained, or shared with third parties.[6] The inconsistent manner in which such information is disclosed to consumers weakens consumer autonomy and undermines trust in digital markets, exposing significant limitations in existing legal frameworks when it comes to addressing exploitative data practices within platform-based commerce. [7]

The NDPA further establishes the Nigeria Data Protection Commission (NDPC) under Section 4 as the principal regulatory body responsible for enforcement. Beyond the principles and lawful bases discussed above, the Act imposes a series of independent obligations that apply regardless of which ground under Section 25 is relied upon. Section 27 requires that data subjects be

[3] O Akinola and O Asaolu, 'A Trust, Privacy and Security Model for E-commerce in Nigeria' *Nigerian Journal of Technology*. (2023) 42(1) 152.

[4] The Nigeria Data Protection Act 2023 Federal Republic of Nigeria Official Gazette No.119 Vol. 110 (1 July 2023).

[5] Balancing data protection with the free flow of information while preventing misuse by third parties remains a challenge. See Z Moric and others 'Protection of Personal Data in the Context of E-Commerce' *Journal of Cybersecurity and Privacy* (2024) 3 731-761

[6] Abiodun Odusote, 'Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation' *Beijing Law Review* (2021) 12(4) 1287, 1290

[7] Ibid, 1290

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

provided with clear information about the processing of their data at or before the point of collection. Section 28 mandates data protection impact assessments for high-risk processing, while Section 29 sets out the general obligations of data controllers and processors. Section 30 imposes heightened requirements for the processing of sensitive personal data, Section 32 requires the appointment of Data Protection Officers in specified circumstances, and Section 40 imposes breach notification obligations.

There is also the Federal Competition and Consumer Protection Act (FCCPA) 2018, [8] which provides a broader consumer protection framework aimed at preventing unfair business practices and protecting consumer welfare, though it is not data-specific in the way the NDPA is. Notable gaps nonetheless persist in the protection of consumer data in Nigeria. These gaps are not necessarily attributable to the absence of legal rules, the NDPA's framework of lawful bases and accompanying obligations is, on its face, reasonably comprehensive. The gaps are attributable to weak enforcement,[9] fragmented regulatory oversight,[10] and the reduction of consent, in practice, to a procedural compliance mechanism by digital platforms, often at the expense of the substantive obligations imposed elsewhere in the Act. This paper discusses the failure of legal rules to provide effective consumer data protection in Nigeria's e-commerce sector. It argues that the principal challenge is not legislative inadequacy but four interlocking institutional failures. First, the absence of a binding coordination mechanism between the NDPC and the FCCPC creates jurisdictional ambiguity: because neither the NDPA nor the FCCPA establishes a clear enforcement hierarchy between the two bodies, platforms can exploit the resulting uncertainty, and complaints risk falling into a regulatory gap rather than triggering a coordinated response .[11] Second, the NDPC's own enforcement capacity is constrained by resource limitations of the reported data breaches in 2024, only a small fraction underwent full investigation, meaning that even well-designed statutory powers translate into a low probability of actual sanction, which in turn does little to deter data-exploitative business models. Third, low consumer awareness of data protection rights suppresses the complaint volume needed to activate enforcement in the first place, since regulators in Nigeria's current model rely heavily on data-subject complaints

[8] Federal Competition and Consumer Protection Act (FCCPA), Official Gazette No 18, Lagos 1 February 2018 Vol 106, Government Notice No 5.

[9] **Stephanie Modilim** and others, **'**Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment**'** *International Journal of Law Management & Humanities* **(**2024) 7(6) 2481 – 2495; Patrick Chukwunonso Aloamaka 'A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms' *UCC Law Journal*. (2025) 4(2) Volume, 242-

[10] Asere Gbenga Femi , 'Evaluating the Level of Compliance with the Nigeria Data Protection Regulation (NDPR): Insights from Organizations across Key Sectors' *Journal of Cybersecurity* 382

[11] John Oluyinka Adedeji and Ahmed Osilama Abu, 'An Assessment of the Effectiveness of the Federal Competition and Consumer Protection Commission (FCCPC) on Consumer Rights Protection in E-Commerce Transactions in Nigeria' *Journal of Business Development and Management Research* (2025) 8(7) 36.

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

rather than proactive supervision .[12] Fourth, consent under the NDPA has been reduced to a procedural compliance mechanism: platforms rely on bundled, lengthy privacy policies. As such, this paper scrutinises the gap between Nigeria's formal data protection regime and the realities of platform-based commerce, especially with respect to consumer autonomy, transparency, and efficacy of enforcement.[13].[14]

The thesis of this paper is that Nigeria's consumer data protection regime in e-commerce is undermined primarily by institutional and enforcement deficiencies rather than by the absence of legal principles. Although the NDPA 2023 and the FCCPA 2018 establish important regulatory standards, their effectiveness is weakened by the same four institutional failures identified above: jurisdictional ambiguity between the NDPC and the FCCPC, constrained NDPC enforcement capacity, low consumer awareness that suppresses complaint-driven enforcement, and the reduction of consent to a procedural compliance mechanism. Consequently, this paper contends that meaningful consumer data protection in Nigeria requires a transition from procedural compliance toward coordinated, enforcement-driven regulation that prioritizes substantive consumer rights and platform responsibility.

This paper proceeds in several stages. Following this introduction, the methodology section explains the doctrinal and comparative legal approach adopted, while the next section examines the legal and regulatory framework governing consumer data protection in Nigeria. The paper proceeds to analyse platform accountability with a case study investigation of the privacy policies of selected leading e-commerce platforms operating in Nigeria with an emphasis on transparency, consent mechanisms, data retention and third-party data sharing practices.

This paper then engages in a comparative analysis of the European Union's General Data Protection Regulation (GDPR) and the enforcement model of the United States Federal Trade Commission (FTC) to identify lessons for strengthening Nigeria's regulatory approach. This

---

12 Iyemeake Sunday and Ireghan Mohammed Mulktaru 'Critical Analysis of Consumers' Rights Under E-Commerce Transactions in Nigeria' *International Journal of Advanced Studies in Economics and Public Sector Management* (2025) 13 71

13 A Muneer, S Razzaq and Z Farooq, 'Data Privacy Issues and Possible Solutions in E-commerce' *Journal of Accounting and Marketing* (2018) 7 294; Concerns about fraud, payment security, and the authenticity of online vendors continue to deter many Nigerians from fully embracing e-commerce. Some authors have also noted that there are concerns about the protection of consumers' personal data, which they must inevitably provide to transact business online. For instance, Arora emphasizes the challenges of safeguarding consumer data as e-commerce platforms continue to gain widespread adoption, see D Arora, 'Data Privacy Issues with E-Commerce' *International Journal of Social Science and Economic Research* (2023) 8 1167–1174

14 A Muneer, S Razzaq and Z Farooq, 'Data Privacy Issues and Possible Solutions in E-commerce' *Journal of Accounting and Marketing* (2018) 7 294; Concerns about fraud, payment security, and the authenticity of online vendors continue to deter many Nigerians from fully embracing e-commerce. Some authors have also noted that there are concerns about the protection of consumers' personal data, which they must inevitably provide to transact business online. For instance, Arora emphasizes the challenges of safeguarding consumer data as e-commerce platforms continue to gain widespread adoption, see D Arora, 'Data Privacy Issues with E-Commerce' *International Journal of Social Science and Economic Research* (2023) 8 1167–1174

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

paper subsequently summarises its key findings regarding enforcement fragmentation, weaknesses in consent regulation, low consumer awareness, and limited platform accountability. Finally, the paper concludes by demonstrating that the resolution of Nigeria's consumer data protection challenges depends on stronger institutional coordination, clearer enforcement mandates, improved consent standards, and a more robust system of platform accountability supported by effective regulatory enforcement

2.0 METHODOLOGY

This paper adopts a doctrinal and comparative legal research methodology. Through the doctrinal research methodology, the paper critically examines Nigeria's legal and regulatory framework governing consumer data protection in e-commerce, with particular focus on the Nigeria Data Protection Act (NDPA) 2023, the General Application and Implementation Directive (GAID) 2025,[15] and the Federal Competition and Consumer Protection Act (FCCPA) 2018. This paper also carries out an analysis of relevant judicial decisions, policy materials, and academic literature in order to evaluate the effectiveness of the existing framework.

This paper also adopts a comparative methodology by analysing certain components of the European Union General Data Protection Regulation (GDPR) [16] and the United States Federal Trade Commission (FTC) enforcement mechanism. These jurisdictions represent a clear contrast between two major regulatory philosophies in the digital economy.[17] The EU's GDPR represents a broad, rights-based approach where privacy is treated as a fundamental human right. While the United States relies on a more piecemeal, enforcement-heavy system that focuses primarily on consumer protection and preventing unfair business practices.

The comparative dimension of the study is deliberately narrow rather than a general survey of the EU and US regimes, and is confined to the two areas most directly relevant to the institutional failures identified in Nigeria: consent standards and enforcement design. On consent, the study examines Articles 6, 7, and 7(4) of the GDPR, together with the definition of consent under Article 4(11) and the European Data Protection Board's 2020 Guidelines on consent, because these provisions articulate the "freely given, specific, informed, and

---

15 Nigeria Data Protection Act (NDP Act) 2023 General Application And Implementation Directive (GAID) 2025 NDPC/NDP Act-GAID/01/2025 <https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf> accessed 30 December 2025

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (Hereafter referred to as GDPR)

17 Olivia Gavzie, 'The United States Should Adopt a Comprehensive Data Privacy Law Similar to the European Union's GDPR' < https://www.hofstrajibl.org/2026/03/the-united-states-should-adopt-a-comprehensive-data-privacy-law-similar-to-the-european-unions-gdpr/> accessed 13 May 2026

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

unambiguous" standard and the prohibition on bundled consent, a standard against which the NDPA's silence on granularity and bundling can be directly measured. On enforcement, this paper examines the GDPR's administrative fining structure under Article 83 and, on the US side, the FTC's consent-order and civil-penalty powers under Sections 5, 6, and 13(b) of the Federal Trade Commission Act, illustrated through the 2019 Facebook order (US$5 billion, for violating a prior consent order on user control over personal data)[18] and the 2019 Google/YouTube settlement (US$170 million, for collecting children's data without parental consent under COPPA). [19]

These enforcement examples were selected because they involve the same categories of harm this paper identifies in the Nigerian context; misleading platform representations about user control, and non-consensual data collection, allowing a like-for-like assessment of whether Nigeria's statutory penalty ceilings and enforcement practice under the NDPA and FCCPA provide comparable deterrence. The criteria applied throughout the comparison are: (i) the specificity and enforceability of the consent standard; (ii) the size and credibility of the deterrent sanction relative to platform revenue; and (iii) the existence of a single, adequately resourced enforcement authority as opposed to fragmented or overlapping mandates.

A qualitative assessment of the privacy policies of two leading e-commerce platforms operating in Nigeria was also carried out. The two platforms were purposively selected from among Nigeria's highest-traffic e-commerce websites, using publicly available web-traffic rankings and market-share estimates as a proxy for the volume of consumer data each platform is likely to process; platforms without a Nigeria-specific, publicly accessible privacy policy in English were excluded. The privacy policies were retrieved and reviewed in February 2025. Each policy was assessed against a coding framework derived from the NDPA 2023, comprising five categories: (i) transparency of disclosure (whether the purpose, scope, and legal basis of processing are stated in plain, specific terms, per Section 27); (ii) consent mechanism (whether consent is granular, unbundled, and separately obtained for distinct processing purposes, per Sections 25–26); (iii) third-party data sharing (whether specific categories of recipients and purposes of onward transfer are identified, per Section 27(1) (c) and 34(1) (iii)); (iv) data retention (whether a defined retention period or deletion trigger is stated, per Section 24(1)(d)); and (v) consumer control (whether mechanisms for withdrawal of consent, access, and erasure are described and operationally accessible, per Sections 34–36). Each category was scored as disclosed, partially disclosed, or not disclosed, based on the express wording of the policy.

---

[18] Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook' (24 July 2019) <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> accessed 21 February 2025

[19] Federal Trade Commission, 'Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law' (4 September 2019) <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law> accessed 21 February 2025

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

3.0 THE LEGAL AND REGULATORY FRAMEWORK

The Nigeria Data Protection Act (NDPA) 2023 and the Federal Competition and Consumer Protection Act (FCCPA) 2018 constitute the principal legal instruments governing the collection, processing, and use of consumer data in online transactions.

3.1 The Nigeria Data Protection Act 2023: Scope and Limits in E-Commerce

The NDPA 2023 enshrines some of the important principles related to data protection, including lawfulness, fairness, transparency, purpose limitation, data minimization, and security,[20] creating the Nigeria Data Protection Commission (NDPC) as the key supervising body. [21] Such rules apply to e-commerce platforms, which are known to process huge amounts of consumer data. In the NDPA 2023, consent is one of the legal grounds for processing personal data; [22] however, in the context of e-commerce platforms, consent is usually given through very lengthy and complicated policies, which are hardly understood by consumers.[23] Consequently, the consent is more of a procedural tool for compliance rather than an authentic reflection of consumer autonomy. Such an arrangement makes the NDPA less effective when protecting consumer rights, consumers often face limited options when engaging with dominant market participants.

Secondly, although the NDPA contains certain requirements, such as appointing Data Protection Officers, conducting compliance audits, and breach notifications, they are more procedural in nature. [24] There is little guidance within the NDPA regarding the implementation of the duties that are required to be carried out within e-commerce, which involves profiling, behavioral advertising, and third party data transfers. The absence of sector-specific regulatory codes or binding guidelines leaves platforms with wide discretion in interpreting compliance requirements.

Third, although the NDPA grants the NDPC enforcement powers, including the ability to issue compliance orders and impose financial penalties, the deterrent effect of these sanctions against large digital platforms remains uncertain. Section 48 of the NDPA sets penalties at the higher of ₦10 million or 2% of "annual gross revenue of the preceding financial year" for data controllers and processors of major importance, and the higher of ₦2 million or 2% of annual gross revenue for others. The Act does not specify whether "annual gross revenue" refers to the revenue of the Nigerian entity or subsidiary through which a multinational platform operates, or to the global turnover of its parent group, a distinction the GDPR resolves explicitly by basing its equivalent

---

20 NDPA 2023, s 24

21 ibid, s 4

22 Ibid, s 26

23 Xiaodong Ding and Hao Huang,;For Whom is Privacy Policy Written? A New Understanding of Privacy Policies' *Computer Law & Security Review* (2024) 55 <https://doi.org/10.1016/j.clsr.2024.106072> accessed 1 September 2026

24 Ibid, s 32, s 33, s 40

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

fines on the "total worldwide annual turnover" of the undertaking.[25] This ambiguity in the NDPA has not yet been tested against a major global platform: the NDPC's only large-scale enforcement action to date, the $220 million penalty against Meta, was imposed by the FCCPC under its separate competition and consumer-protection powers rather than under the NDPA's revenue-percentage formula, meaning the NDPA's own penalty ceiling remains largely unexercised in practice against platforms of this scale.[26] Until that formula is applied to a case of comparable magnitude, it is not possible to say with certainty whether "annual gross revenue" would be read to capture only local revenue, which for a multinational platform may be a small fraction of what it earns worldwide, or the revenue of the global undertaking; the former reading would risk precisely the kind of diluted deterrence this section describes.

Beyond the design of the penalty ceiling, the NDPC's capacity to enforce it at scale is itself constrained. The Commission 'faces challenges in enforcing compliance due to insufficient manpower and technical resources.'[27] Low public awareness compounds this problem, as many Nigerians do not know how to lodge complaints with the NDPC in the first place.[28]

3.2 Overview of the Federal Competition and Consumer Protection Act (FCCPA)

The FCCPA 2018 provides a broader consumer protection framework aimed at preventing unfair, deceptive, and anti-competitive business practices.[29] Although the Act does not expressly regulate data protection, several provisions are capable of capturing data-related harms as unfair or deceptive practices. Section 127 renders void any contract term that is excessively one-sided, based on misleading representations, or not clearly brought to the consumer's attention a standard squarely applicable to bundled or buried consent clauses in a platform's privacy policy. Section 128 requires that any notice imposing an obligation on the consumer be conspicuously disclosed, with adequate opportunity to understand it before the transaction, while Section 129 voids any term that misleads consumers or causes them to waive their rights. Section 125 separately prohibits false, misleading, or deceptive representations, and Section 17 empowers the FCCPC to investigate and eliminate such conduct. The Commission may investigate, sanction, and issue corrective orders under Sections 146 to 155.

The jurisdictional relationship between the FCCPC and the NDPC has not been resolved by statute, neither the FCCPA nor the NDPA establishes an express coordination mechanism

---

25 GDPR, art 83(4)–(6) (referring to "total worldwide annual turnover of the preceding financial year").

26 FCCPC 'Violation: Tribunal Upholds FCCCPC's $220m Fines against Meta/Whatsapp' < https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/> accessed 9 September 2026

27 Kareem Lawal 'The Role of the Nigeria Data Protection Commission (NDPC) in Strengthening Data Privacy Regulations' <https://www.researchgate.net/publication/390890921_The_Role_of_the_Nigeria_Data_Protection_Commission_NDPC_in_Strengthening_Data_Privacy_Regulations> accessed 9 September 2026

28 ibid

29 FCCPA 2018, s 1

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

between the two bodies, but it has been tested in practice. In the FCCPC's action against Meta and WhatsApp, the Competition and Consumer Protection Tribunal held that the Commission acted within its statutory mandate under Section 104 of the FCCPA, which empowers it to regulate consumer protection even in regulated industries, and separately upheld the Commission's finding that Meta's privacy policy violated Nigerian law.[30] This suggests that the FCCPC's consumer-protection powers can, in principle, address data-related harms even in the absence of explicit statutory privacy provisions, though the absence of a codified coordination framework between the FCCPC and the NDPC leaves this jurisdictional overlap capable of recurring in future cases without a settled statutory answer.

The FCCPC Act does not however address data privacy concerns in detail, so while complaints can be filed under the Act, enforcement may be limited to broader consumer protection rules rather than specific data privacy laws. While consumers have the right to escalate complaints, the enforcement of resolutions depends on the effectiveness of the FCCPC or relevant regulators, which may sometimes face resource or other constraints as seen with the NDPC.

3.3 Regulatory Overlap and Enforcement Fragmentation

A weakness in Nigeria's consumer data protection framework lies in the overlapping mandates of the NDPC and the FCCPC. The NDPC is the primary authority for enforcing data protection obligations under the NDPA 2023, and Section 63 of the NDPA gives the Act priority over other legislation on data protection matters to the extent of any inconsistency. The FCCPA 2018 contains a comparable priority clause in its own domain: Section 104 establishes the FCCPC as the primary authority on competition and consumer protection across all sectors, while Section 105 provides for concurrent jurisdiction with sector regulators and requires a coordinated approach under Section 105(3), with the FCCPC empowered to negotiate formal coordination agreements under Section 105(4). These are not, therefore, two agencies operating without any statutory hierarchy; each statute establishes priority within its own subject matter. The difficulty is that neither Act specifies which hierarchy governs where a single practice, such as a platform's privacy policy, falls within both domains at once. In *Nnubia v Hon. Minister Of Industry, Trade & Investment & 2 Ors*[31] the court addressed an analogous overlap between the FCCPA and the Nigerian Communications Act, holding that the FCCPA prevails as the later statute but that the FCCPC and the sector regulator hold concurrent jurisdiction with a duty to coordinate.[32] That reasoning has not been tested as between the FCCPC and the NDPC specifically, so it remains unclear whether a court would resolve a data-related dispute the same way. In practice, the two

---

30 FCCPC 'Violation: Tribunal Upholds FCCCPC's $220m Fines against Meta/Whatsapp' < https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/> accessed 9 September 2026

31 (2025) 4 CLRN < https://clrndirect.com/product/nnubia-v-hon-minister-of-industry-trade-investment-2-ors/>

32 FCCPC 'FCCPC Floors MTN: Court Affirms Its Regulatory Authority in the Telecommunications Sector' < https://fccpc.gov.ng/fccpc-floors-mtn-court-affirms-its-regulatory-authority-in-the-telecommunications-sector/> accessed 9 September 2026

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

commissions have proceeded by cooperation rather than by resolving the statutory question: the FCCPC and NDPC conducted the Meta investigation jointly.

In the past, both bodies have collaborated to handle data breach cases, but these cases do not occur regularly.[33] A formal codification of the framework for enforcement will ensure that all avenues for platforms to take advantage of regulatory ambiguity are closed. The laws in Nigeria provide a framework for the protection of consumer data in Nigeria, however, there are some gaps which hinders enforcement. For instance, the formalistic reliance on consent as a regulatory safeguard, limited deterrent enforcement mechanisms, and fragmented institutional oversight.

Secondly, the level of awareness of data protection rights in Nigeria is low, even where consumers are aware of their rights, there is no active engagement with the privacy policies or even the exercise of rights.[34] This means the consumers are also unaware of the risks involved. Nigerian consumers tend to prioritise financial data security, such as protection against payment fraud, while underestimating the risks associated with non-financial personal data, including location data, browsing behaviour, and digital identifiers.[35] This narrow perception weakens the protective intent of the NDPA, which recognises personal data broadly and grants data subjects rights of access, rectification, erasure, and withdrawal of consent.[36] Where consumers are unaware of these rights, the regulatory framework risks becoming ineffective in practice. The consequence is a persistent trust deficit;[37] many consumers are hesitant to share personal information online due to fears of identity theft, unauthorised data sharing, and data breaches.[38]

---

33 See, Federal Competition and Consumer Protection Commission, *Final Order and Notice Pursuant to Joint Investigation with Nigeria Data Protection Commission* (18 July 2024). <https://fccpc.gov.ng/wp-content/uploads/2024/07/Final-order-FCCPC-Meta-18072024.pdf> accessed 20 February 2025; see also, FCCPC, 'In the Matter of Investigation into Possible Violations of the Rights of Nigerian Consumers in the Provision of Contact-Based Instant Messaging Service in Nigeria and Enquiries into Obnoxious, Exploitative, and Unscrupulous Business Practices by Whatsapp Llc and Meta Platforms, Inc. under the Federal Competition and Consumer Protection Act, 2018 ' <https://fccpc.gov.ng/wp-content/uploads/2024/07/Excutive_Summary-_WhatsApp_Investigation-13.11.23.pdf> accessed 19 February 2025

34 Oluwafemi Osho, 'E-Commerce in Nigeria: A Survey of Security Awareness of Customers and Factors that Influence Acceptance' <https://www.researchgate.net/publication/311589556_E-Commerce_in_Nigeria_A_Survey_of_Security_Awareness_of_Customers_and_Factors_that_Influence_Acceptance> accessed 24 February 2025

35 Tiwalade Adelola, Ray Dawson, Firat Batmaz, 'Nigerians' Perceptions of Personal Data Protection and Privacy' <https://www.researchgate.net/publication/275968129_Nigerians'_Perceptions_of_Personal_Data_Protection_and_Privacy?__cf_chl_tk=nKU5IvNvP79D4o_icZ8omoIoDWKoxDJlK_c_BEYu85w-1740395647-1.0.1.1-m.ocXtRDInvWMPltZXpUMrBpL1Ku5k7_e4ntzNQfv_k> accessed 24 February 2025

36 NDPA 2023, s 35-36

37 Iyemeake Sunday and Ireghan Mohammed Mulktaru, *International Journal of Advanced Studies in Economics and Public Sector Management* (2025) 13(1) 65

38 Goodhead T. Abraham, 'Usability, Security and Trust of E-commerce Websites: The Effect on the Nigerian E-Shopper' *Asian Journal of Research in Computer Science* (2021) 10(4) 58-68

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

This distrust undermines consumer confidence in digital markets and highlights the limitations of rights-based data protection regimes in low-awareness environments.

4. PLATFORM ACCOUNTABILITY AND DATA SECURITY PRACTICES IN NIGERIA'S E-COMMERCE SECTOR

Platform accountability is an important element of effective consumer data protection in e-commerce. This section examines the privacy policies of Jumia and Konga, two leading e-commerce platforms operating in Nigeria, across four areas: transparency and accountability, security safeguards, user control mechanisms, and data retention practices, assessed against the requirements of the NDPA 2023..[39]

4.1 Transparency and Accountability in Platform Data Practices

Transparency is a foundational principle of data protection under the NDPA. Section 27 requires that data subjects be given clear and accessible information about how personal data is collected, used, shared, and retained. [40] Jumia's privacy notice sets out a developed transparency framework: it separately identifies four lawful bases for processing (consent, legitimate business interest, contract performance, and legal compliance), specifies detailed categories of data collected (including biometric and financial data), and names categories of third-party recipients, fulfilment and delivery partners, payment processors, advertisers, and, in specified circumstances, an acquiring business in the event of a merger alongside a general purpose for each category.[41] Jumia also names the Nigeria Data Protection Commission (NDPC) as the body to which a user may escalate a complaint. Konga's privacy policy is markedly less developed on this measure. It lists purposes for processing (order fulfilment, service improvement, marketing, fraud prevention, legal compliance) without organising these around distinct lawful bases; only marketing is expressly tied to consent, leaving the legal basis for the remaining purposes unstated.[42] Konga does, however, make one specific and checkable commitment that Jumia's policy does not: an express statement that it does "not sell, trade, or rent" personal information to third parties. Beyond this, Konga names only broad categories of recipients (service providers, legal authorities, business partners) without Jumia's level of purpose-specific detail, and its policy contains no reference to the NDPC or any external complaint or escalation route. Neither

---

39 The privacy policies of two leading e-commerce platforms operating in Nigeria, Jumia and Konga, are examined, with the focus on four core areas: transparency and accountability, security safeguards, user control mechanisms, and responsiveness to data protection risks, assessed against the requirements of the NDPA 2023. The two platforms were selected as among the highest-traffic e-commerce sites operating in Nigeria, and their privacy policies were reviewed as publicly available documents in [insert month/year]. The assessment that follows describes what each policy discloses, or fails to disclose, against the NDPA's requirements; it is not a finding that either platform has violated the Act, since such a finding falls within the exclusive competence of the NDPC or a court.

40 NDPA s 27

41 Jumia Privacy Notice (Version 3, dated 21 February 2025 < https://vendorhub.jumia.com.ng/jumia-privacy-notice/> accessed February 2025);

42 Konga Privacy Policy, < https://www.konga.com/content/privacy-policy> accessed 9 September 2026

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

policy names the specific third-party companies with which data is shared, nor specifies which categories of personal data go to which recipient. This falls short of full transparency even where the letter of Section 34's "categories of recipients" language may be technically satisfied; since a data subject reading either policy cannot determine which specific organisations hold their data.

4.2 Data Security Measures and Risk Management

Data controllers are obligated to implement appropriate technical and organisational measures to ensure the security of personal data. Encryption, secure communication protocols, multi-factor authentication, and internal access controls are some of these measures.[43] Data controllers are obligated to implement appropriate technical and organisational measures to secure personal data. Jumia's policy commits to limiting access to personal data on a need-to-know basis among employees, agents, and contractors, and separately commits to a breach-notification procedure "where legally required." Konga's policy states only that it implements "appropriate security measures" against unauthorised access, alteration, disclosure, or destruction, adding the standard caveat that no method of internet transmission is completely secure; it does not commit to any breach-notification procedure, nor does it describe any access-control measure. Neither policy specifies particular technical safeguards, such as encryption standards, two-factor authentication, or a defined access-control architecture that would allow a data subject to independently assess the strength of protection actually applied to their data.

Generally, platforms need to be more transparent about how consent is obtained, particularly for sensitive data or data sharing with third parties, data retention periods, and the use of cookies and tracking technologies. The GAID 2025 is instructive here: Article 19 requires conspicuous cookie banners and opt-in consent for most tracking tools, while Article 19(5) exempts necessary cookies from the active tick-box requirement. Read alongside Article 17(8)(b), which treats the mere closing of a privacy notice as implied consent, this creates a gap: a platform can remain technically compliant while a user's dismissal of a banner, done simply to see the page, is treated in law as consent to tracking..

The risks associated with third-party data sharing are further illustrated by the 2025 judicial decision in *Araka v. Ecart Internet Services Nig. Ltd. & Anor.*[44] In which a customer who had

[43] Harson Kapoh and other 'Data Security and Data Protection in Cloud Privacy Systems' (2024) 5(11), Syntax Admiration, 4801; Amirul Hakim and others, 'Firewalls, Intrusion Detection/Prevention, Encryption, and Multi-Factor Authentication In Cybersecurity Solutions' 1 <https://www.researchgate.net/publication/382596527_FIREWALLS_INTRUSION_DETECTIONPREVENTION_ENCRYPTION_AND_MULTI-; Maha Sayal, Mali Alameady and Salah Albermany, 'The Use of SSL and TLS Protocols in Providing a Secure Environment for e-commerce Sites'<https://www.researchgate.net/publication/347826412_The_Use_of_SSL_and_TLS_Protocols_in_Providing_a_Secure_Environment_for_e-commerce_Sites> accessed 24 February 2025

[44] (Suit No. FHC/ABJ/CS/195/2024, Federal High Court, Abuja, 18 February 2025)

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

ordered through Jumia Food a now-discontinued food-delivery service, distinct from the core Jumia e-commerce platform reviewed in this paper began receiving unsolicited marketing messages from the restaurant vendor after his order was fulfilled through Ecart, the delivery intermediary. The court held that the unauthorised use of the applicant's data for direct marketing breached his right to privacy under Section 37 of the 1999 Constitution and the NDPA's purpose limitation principle, ordered the erasure of his data and a permanent injunction against further marketing use, and awarded ₦3,000,000 in damages. The case demonstrates that data collected for one purpose (order fulfilment) can be repurposed for another (marketing) once shared with a third party, precisely the kind of downstream use that the category-level disclosures in Jumia's and Konga's own policies do not allow a user to trace or prevent.

4.3 User Control, Consent Withdrawal, and Data Retention Practices

User control is a core element of data protection under the NDPA. NDPA requires the process for withdrawal to be as easy as the process for granting consent, data subjects should be able to withdraw consent without any condition.[45] Withdrawal of consent is distinct from erasure: withdrawing consent removes the legal basis for future processing, but does not by itself require the controller to delete data already held, particularly where the data continues to be needed for a purpose resting on a different lawful basis, such as a legal retention obligation or a legitimate business interest. Erasure is a separate right under Section 34, and a data subject who wants their data deleted, rather than merely stopping its future use, must exercise that right specifically. This distinction matters where a platform's processing rests on multiple lawful bases at once: withdrawing consent to marketing use, for example, does not require the platform to stop processing the same data where that processing is separately justified by contract performance (such as fulfilling an order) or a legal obligation (such as tax recordkeeping). The two policies differ in how they frame self-service control. Jumia allows a user to opt out of personalisation or marketing by closing their account or by emailing its Data Privacy Officer, and separately allows account deletion through a dedicated "Delete Account" feature; it reserves the right to refuse a request that is unreasonable or inadequately verified. Konga's policy states, more simply, that a user may "access, update, or delete" personal information "at any time" and may manage preferences and communications settings "in your account dashboard," a framing that, if the dashboard functions as described, is a more self-service-oriented mechanism than Jumia's for that specific purpose. Neither policy, however, describes a comparable self-service mechanism for objecting specifically to third-party data sharing or behavioural tracking; a user wishing to stop these narrower forms of processing must rely on the general contact routes each policy provides, rather than adjust a dedicated setting.

On cookies specifically, the two platforms diverge more sharply. Jumia's website provides a dedicated, categorised cookie preference tool, allowing a user to independently toggle Advertising, Analytics, and Personalisation cookies, separate from the Essential category, which

[45] NDPA 2023, s 35

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

cannot be disabled. Konga's policy states that the only way to control cookies is through the user's own browser settings; it does not describe an on-site preference centre.

Section 24(1)(d) of the NDPA requires that personal data be retained only for as long as necessary for the purposes for which it was collected. Jumia's policy reflects this principle explicitly: retention is tied to the duration of the ongoing relationship, the continued existence of a valid legal basis, and applicable limitation periods, with a stated commitment to delete or anonymise data once no longer needed. Konga's current policy contains no retention provision at all, no stated principle, no linkage to purpose, and no reference to deletion timelines which is a more significant gap than an imprecisely worded retention clause; it is the absence of one. This asymmetry between the two platforms means that a Konga user has no basis, from the policy text alone, for knowing how long their data will be kept or on what basis it will eventually be deleted.

5.0 COMPARATIVE INTERNATIONAL BENCHMARKS

This section takes specific lessons from two well-developed examples of regulation in this area, General Data Protection Regulation (GDPR) from the European Union (EU) and the Federal Trade Commission (FTC)[46] from the United States. Instead of attempting to provide a comprehensive overview of how regulations can be implemented effectively in Nigeria, this section will look at two specific issues that are most relevant to the Nigerian context with respect to enforcement design and consent standards.

5.1 European Union's GDPR Enforcement

The GDPR represents the most comprehensive and enforcement-driven data protection regime globally and this makes it relevant to Nigeria.[47] Article 6, requires the processing of personal data to be based on a lawful basis, with consent constituting one such basis where appropriate. Under Article 4(11), consent must be "freely given, specific, informed and unambiguous", while Article 7 establishes additional conditions governing its validity and withdrawal. The European Data Protection Board (EDPB) further explains that valid consent must provide the data subject with genuine choice and control. (EDPB).[48] In particular, consent is unlikely to be freely given where a controller makes the provision of a service conditional upon consent to processing that is not necessary for that service.[49]

This approach is particularly relevant to platform-based e-commerce because it addresses situations in which consumers may have limited bargaining power in relation to digital service providers. Article 7(4) of the GDPR requires particular consideration of whether the performance of a contract is conditional on consent to processing that is not necessary for the performance of that contract (GDPR, art 7(4)). The EDPB therefore emphasizes that consent should not be

---

46 The Federal Trade Commission (FTC) enforces consumer protection laws under **the** Federal Trade Commission Act, 15 **USC § 41 (1914)**

47 Moric and others, (n 5) 731

48 Guidelines 05/2020 on Consent under Regulation 2016/679, paras 13–14

49 Ibid, para 39

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

obtained by bundling distinct processing purposes where the data subject could reasonably be expected to give separate choices.[50] The EDPB's principle of granularity requires that, where processing serves several purposes, data subjects should be able to choose which purposes they accept rather than being required to consent to a bundle of unrelated processing operations.[51]

The same principle applies to cookie walls. Paragraph 39 of the EDPB Guidelines 05/2020 provides that access to services or functionalities must not be made conditional on the user's consent to the storing of information or gaining access to information already stored in the user's terminal equipment. Paragraphs 40–41 illustrate this through a website that blocks access to its content unless the user clicks "Accept cookies"; because the user is not presented with a genuine choice, the consent is not freely given and is therefore invalid. Thus, the EDPB position is not simply that cookie notices should be more transparent; rather, consent cannot be regarded as freely given where access to a service is conditional upon acceptance of non-essential cookies or similar tracking technologies.[52]

The precise lesson for Nigeria is therefore one of substantive consumer choice rather than formal consent. Nigerian e-commerce platforms should not be permitted to make access to essential services conditional upon acceptance of non-essential tracking or unrelated data-processing purposes. The NDPC, working with the FCCPC, should accordingly require platforms to separate processing purposes, provide meaningful choices for non-essential processing, and ensure that refusal of such processing does not result in denial of access to the core service. This would provide a more concrete regulatory response to the concern identified above that Nigerian consumers may be presented with consent mechanisms that appear formally compliant while providing little meaningful control over the use of their personal data.

This comparative lesson is particularly significant in light of the GAID 2025 provisions discussed above. Rather than permitting platform design to determine whether a consumer's conduct amounts to consent, Nigerian regulation should make the existence of a genuine alternative a prerequisite for treating consent as valid. The relevant reform is therefore not to replicate the GDPR wholesale, but to transfer its underlying safeguard against coerced or bundled consent into the Nigerian e-commerce context.

5.2 United States: FTC Enforcement Model

The Federal Trade Commission (FTC) is responsible for ensuring consumer data protection, and preventing unfair or deceptive acts or practices.[53] This general jurisdiction is distinct from the FTC's authority under sector-specific statutes that Congress has separately enacted and tasked

[50] Ibid, paras 42–45)
[51] Ibid
[52] Ibid, paras 39–41
[53] Federal Trade Commission Act s 5

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

the FTC with enforcing, such as the Children's Online Privacy Protection Act (COPPA), which imposes particular notice and parental-consent obligations on operators that knowingly collect data from children under 13.[54] The FTC can investigate, issue consent orders and injunctions, and pursue significant financial penalties under either authority.[[55]

The 2019 action against Facebook illustrates the FTC's general Section 5 authority: the Department of Justice, acting on the FTC's referral, sued Facebook in the U.S. District Court for the District of Columbia for violating a 2012 administrative consent order that had itself been grounded in Section 5's prohibition on unfair and deceptive practices relating to user privacy.[56] The court entered a Stipulated Order imposing a $5 billion civil penalty and additional injunctive privacy requirements.[57] By contrast, the 2019 action against Google and its subsidiary YouTube was brought under COPPA specifically, not under the FTC's general unfairness/deception authority: the FTC and the New York Attorney General jointly alleged that Google and YouTube collected personal data from viewers of child-directed content without providing the notice or obtaining the verifiable parental consent that COPPA requires, resulting in a $170 million civil penalty under a Stipulated Order entered in the same district court.[58]

The distinction matters for what each case shows: Facebook demonstrates the FTC's capacity to impose a substantial penalty using its general, cross-sector mandate once a company breaches a prior commitment, while Google/YouTube demonstrates enforcement under a narrower, subject-specific statute enacted for a particular vulnerable population. Nigeria's framework does not yet have an equivalent sector-specific statute comparable to COPPA; the NDPA operates only at the level of general application, closer in structure to the FTC Act's Section 5 than to COPPA.

The FTC model emphasizes enforcement over formal compliance and this is a lesson Nigeria can learn. Rather than relying primarily on privacy policies and consent documentation, the FTC is concerned with whether platform practices are fair and transparent. This is an outcome-oriented approach which aligns closely with consumer protection principles.

5.3 Lessons for Nigeria's E-Commerce Consumer Protection Framework

---

54 Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.

55 FTC Act, 15 U.S.C. §§ 45(a), 45(l), 53(b), 56(a)(1).

56 *United States v Facebook, Inc.*, Case No. 1:19-cv-02184 (TJK) (D.D.C., complaint filed 24 July 2019); *In re Facebook, Inc.*, FTC File No. 182-3109, Docket No. C-4365 (2012 administrative order).

57 Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v Facebook, Inc.*, No. 1:19-cv-02184 (D.D.C., entered 24 April 2020). < https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf> accessed 9 September 2026

58 Complaint, *United States v Google LLC and YouTube, LLC*, Civil Action No. 1:19-cv-02642 (D.D.C., filed 4 September 2019), FTC File No. 172-3083; Stipulated Order for Permanent Injunction and Civil Penalty Judgment, same case (entered 10 September 2019). < https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf> accessed 9 September 2026

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

An important lesson from the comparative analysis is that effective consumer data protection depends not merely on the existence of broad legal principles, but on the institutional capacity to translate those principles into effective enforcement. The comparison with the GDPR and the United States therefore supports specific reforms to Nigeria's enforcement architecture. First, the GDPR demonstrates the importance of linking the severity of sanctions to the nature, gravity and duration of the infringement, the number of data subjects affected the level of harm and the economic circumstances of the undertaking. Article 83(1) requires administrative fines to be effective, proportionate and dissuasive, while Article 83(2) requires these and other factors to be considered in determining the appropriate penalty.

For Nigeria, this supports a more systematic application by the NDPC of the factors already contained in Section 48 of the NDPA when determining penalties against major e-commerce platforms. The objective should be to ensure that penalties reflect both the seriousness of the violation and the economic capacity of the offending platform, rather than treating the statutory maximum as an automatic or uniform penalty.

Second, the GDPR demonstrates that financial penalties need not operate in isolation from other enforcement measures. Supervisory authorities may combine fines with corrective measures, including orders requiring controllers or processors to comply with the Regulation or to restrict or suspend processing.[59] This supports the strengthening of the NDPC's use of corrective and remedial measures alongside financial penalties, particularly where an e-commerce platform continues to employ unlawful consent mechanisms, excessive data collection or other practices that expose consumers to continuing harm. The reform supported by the EU comparison is therefore not simply an increase in fines, but a more graduated enforcement strategy in which financial penalties are accompanied, where appropriate, by binding corrective orders.

Third, the United States provides a complementary lesson concerning the use of negotiated and continuing enforcement orders. The Federal Trade Commission has used privacy and data-security enforcement actions to require companies to implement comprehensive privacy and security programmes, submit to independent assessments, delete unlawfully obtained information and undertake other remedial measures.[60] This suggests that Nigerian enforcement should not end with the imposition of a monetary penalty. Where an e-commerce platform has engaged in serious or repeated violations, the NDPC, in appropriate cases and within its statutory powers, should require verifiable remedial measures, including modification of data-handling practices, deletion or restriction of unlawfully obtained data, and continuing compliance monitoring.

---

59 GDPR 2016, art 58(2); art 83(2)

60 FTC, 'The Federal Trade Commission 2023 Privacy and Data Security Update' <https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.21-PrivacyandDataSecurityUpdate-508.pdf> accessed 9 September 2026

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

The comparative analysis therefore supports three specific institutional reforms in Nigeria: **(1)** more systematic and proportionate application of Section 48 of the NDPA by the NDPC, taking account of the scale of the platform, the number of consumers affected and the gravity and duration of the breach; **(2)** greater use of corrective orders alongside financial penalties to stop continuing unlawful processing; and **(3)** stronger post-enforcement compliance mechanisms for serious or repeated violations, drawing on the remedial and continuing-order approach evident in US consumer privacy enforcement. These reforms would make the Nigerian enforcement framework more capable of imposing consequences that are meaningful to economically powerful platforms while remaining proportionate to the circumstances of each case. The comparative lesson is therefore not that Nigeria should replicate the GDPR or the US enforcement model, but that the NDPC should move from predominantly formal compliance towards a more graduated, harm-sensitive and outcome-oriented enforcement approach.

6.0 SUMMARY OF FINDINGS

This paper advances the following six findings, each derived from the statutory and case-study analysis set out above and substantiating the three mechanisms identified in the conclusion: Findings 1 and 6 substantiate the jurisdictional-ambiguity and deterrence mechanisms; Findings 3 and 4 substantiate the platform-accountability gaps documented in the case study; Finding 2 substantiates the procedural-consent mechanism; and Finding 5 illustrates the practical consequence of the enforcement-capacity mechanism.

1. Nigeria's data protection framework contains two domain-specific statutory hierarchies that do not resolve conflicts arising at their intersection. Section 63 of the NDPA establishes the Act's priority over other legislation on data protection matters, while Section 104 of the FCCPA establishes the FCCPC's priority on competition and consumer protection matters across all sectors. Because a single practice, such as a platform's privacy policy, can fall within both domains simultaneously, neither statute's priority clause resolves which body should act first. The Federal High Court's reasoning in *Nnubia v Minister of Industry, Trade and Investment* addressed an analogous overlap between the FCCPA and the Nigerian Communications Act by finding concurrent jurisdiction with a duty to coordinate, but this reasoning has not been tested between the FCCPC and the NDPC specifically, leaving the question unresolved in practice.
2. Consent operates as a procedural formality rather than a substantive safeguard, a pattern traceable to a specific interaction between two GAID provisions. Article 19(5) of the GAID exempts necessary cookies from the active opt-in requirement, while Article 17(8)(b) treats the mere closing of a privacy notice as implied consent. Read together, these provisions allow a platform to remain technically compliant while a user's dismissal of a banner done simply to view a page is treated in law as consent to tracking. This is consistent with the case-study finding that neither Jumia's nor Konga's policy allow a user to grant or withhold consent to third-party sharing or behavioural tracking independently of broader account settings.
3. Platform disclosure of third-party data sharing and retention practices falls short of the transparency the NDPA requires, though the gap differs in degree between platforms. The case-study review found that both Jumia and Konga disclose categories of third-party recipients

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

without naming the specific organisations involved , which limits a data subject's ability to trace who holds their data notwithstanding technical compliance with Section 27 and Section 34. On retention, the gap is more pronounced for Konga, whose current policy contains no retention provision at all, compared with Jumia's policy, which ties retention to purpose, relationship duration, and applicable limitation periods in line with Section 24(1)(d).

4. Stated security commitments are not verifiable from the policy text, independent of which platform is at issue. Both Jumia's and Konga's policies commit only to general organisational measures: access limitation and undefined "security measures," respectively, without specifying technical safeguards such as encryption standards or two-factor authentication. This means a data subject has no way to assess, from the policy itself, the actual strength of protection applied to their data.

5. Judicial enforcement of data rights has occurred, but through private litigation rather than regulatory action, which raises a separate access-to-justice concern. *Araka v Ecart Internet Services Nigeria Limited & Eat 'N' Go Limited* demonstrates that a Nigerian court will enforce the NDPA's purpose limitation principle and award damages for unauthorised secondary use of data . That the vindication of this right required an individual to litigate, rather than resulting from proactive regulatory enforcement by the NDPC, is consistent with the resource and capacity constraints on the NDPC identified in section 3.1, and suggests that meaningful redress may depend on a data subject's capacity and willingness to bring a claim.

6. The NDPA's penalty structure contains an unresolved statutory ambiguity that has not yet been tested against a platform of significant scale. Section 48 sets penalties as a percentage of "annual gross revenue" without specifying whether this refers to local or global turnover, unlike the GDPR's express reference to "total worldwide annual turnover". The NDPC's largest enforcement outcome to date, the penalty against Meta, was imposed by the FCCPC under separate statutory powers rather than under this formula, meaning the ambiguity remains untested. The comparative analysis of GDPR's proportionality factors under Article 83 and the FTC's use of continuing compliance orders (section 5) suggests that resolving this ambiguity, and pairing financial penalties with corrective orders, would strengthen the NDPC's capacity to impose consequences proportionate to a platform's scale.

7.0 CONCLUSION

This paper set out to explain why consumer data protection in Nigeria's e-commerce sector remains weak despite the existence of the NDPA 2023 and the FCCPA 2018. The four institutional failures identified in the introduction cluster into three connected mechanisms for the purposes of this synthesis, since low consumer awareness and the NDPC's resource constraints both operate as a single enforcement-capacity problem: awareness determines how many complaints reach the Commission, and resourcing determines how many of those complaints can be acted on, but neither is independently sufficient to explain the enforcement gap without the other. The evidence assembled across the preceding sections supports a specific

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

version of that explanation: the weakness is institutional rather than legislative, and it operates through three connected mechanisms rather than a single cause.

First, the statutory analysis in section 3.3 showed that the NDPC's and FCCPC's respective priority clauses under Section 63 of the NDPA and Section 104 of the FCCPA each resolve hierarchy only within their own domain, leaving practices that straddle both such as a platform's privacy policy without a settled answer as to which regulator leads. This is not a hypothetical gap: the Meta enforcement action proceeded through the FCCPC's general powers rather than the NDPA's own penalty formula (section 3.1), meaning that formula remains untested against a platform of comparable scale, and the ambiguity in "annual gross revenue" identified there has yet to be resolved by an actual case.

Second, the case-study review of Jumia's and Konga's privacy policies (section 4) showed this institutional weakness translating into concrete disclosure gaps at the platform level: neither policy names the specific third parties with which data is shared, Konga's policy contains no retention provision beyond the GAID's six-month statutory backstop, and neither platform's security commitments are specific enough for a data subject to verify independently. These are not failures of drafting alone; they are the practical result of a framework evidenced in section 3.1's discussion of NDPC resourcing with limited capacity to audit disclosure quality across the sector.

Third, the interaction between Article 19(5) and Article 17(8)(b) of the GAID (section 4.2) demonstrates how consent has been structured as a procedural formality: a platform can remain technically compliant while a user's dismissal of a banner is treated in law as consent to tracking. *Araka v Ecart Internet Services Nigeria Limited & Eat 'N' Go* Limited confirms that Nigerian courts will enforce the purpose limitation principle where this formality is breached, but that this vindication depended on individual litigation rather than the routine regulatory action that the NDPC's resource constraints make difficult to sustain at scale (section 3.1).

The comparative analysis in section 5 clarifies what these three mechanisms are missing, rather than proposing that Nigeria adopt either model wholesale. The GDPR's requirement that consent not be conditioned on unrelated processing, and the FTC's use of continuing compliance orders alongside monetary penalties, both address the same underlying problem this paper identifies in Nigeria: a gap between the existence of a legal standard and the institutional capacity to make that standard bind in practice against parties with greater bargaining power than the consumers the standard is meant to protect.

Taken together, the statutory ambiguity in enforcement hierarchy, the disclosure gaps evident in platform practice, and the structural incentive toward procedural rather than substantive consent are not three separate problems but three expressions of the same institutional deficit identified at

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

the outset of this paper: Nigeria's data protection regime is not undermined by an absence of rules, but by the gap between what those rules require on paper and what current institutional capacity can make platforms actually do..

The following five recommendations correspond directly to the institutional mechanisms identified in sections 3 and 4, and are set out below:

1. **Joint Enforcement Coordination:** The existing NDPC–FCCPC memorandum of understanding should be formalised into a binding coordination agreement under section 105(4) of the FCCPA, which already empowers the FCCPC to negotiate coordination agreements with sector regulators, read along Section 61 of the NDPA, which empowers the NDPC to make regulations in furtherance of its functions. The agreement should specify a jurisdictional allocation test rather than leave lead-agency status to ad hoc negotiation: where the alleged harm concerns the lawfulness of the processing itself (absence of a lawful basis, breach of a data protection principle), the NDPC should lead; where the harm concerns market conduct or a false or misleading representation to consumers, the FCCPC should lead; where both elements are present, as in the Meta investigation, the agreement should require a joint investigation with the NDPC directing data protection remedies and the FCCPC directing consumer protection and competition remedies. The joint enforcement task force itself is not something either statute currently authorises as a standing body, so it cannot be created by directive alone. The appropriate instrument is a formal Joint Enforcement Protocol, executed under Section 105(4) of the FCCPA and Section 61 of the NDPA, with each body issuing a corresponding instrument on its own statutory authority, since neither Act gives either regulator power to bind the other unilaterally. The Protocol would establish the task force's composition, meeting cadence, and the jurisdictional test above, and would need to be published by both agencies to be enforceable as a matter of legitimate expectation against platforms, even though it would not itself have the force of primary legislation. A single digital complaints portal, hosted on the NDPC's existing registration and CAR-filing infrastructure under Article 10 of the GAID, should be extended to accept complaints for automatic routing to the lead agency under this test, rather than requiring a complainant to identify the correct regulator themselves. Nigeria can learn from the United Kingdom, which has the Digital Regulation Cooperation Forum (DRCF). This body serves as a benchmark for institutional cooperation, uniting four primary regulators to harmonize their oversight of the digital economy.[61] It has a joint secretariat and annual work plans to ensure that privacy and competition enforcement are harmonized rather than handled in isolation.[62]

[61] See 'DRCF Terms of Reference' <https://www.drcf.org.uk/siteassets/drcf/home/drcf-terms-of-reference.pdf?v=379416> accessed 30 December 2025

[62] ibid

PRINT ISSN: 0794-0254
ONLINE: E-ISSN: 0794-084X

2. **Prohibition on Cookie Walls and Mandatory Choice Symmetry**: The NDPC and FCCPC need to go a step further than the general rules in the GAID. They should co-issue a Guidance Note on Digital Commerce that specifically removes gray areas in the e-commerce sector. Specifically, this needs to ban cookie walls where a consumer is blocked from a site unless the consumer agrees to tracking and bundled consent, where agreeing to one service forces a consumer into a dozen other data-sharing deals. This reform is substantiated by the EDPB's Guidelines 05/2020, paragraphs 39–41, access to a service must not be made conditional on acceptance of non-essential tracking, because consent obtained under such conditions is not freely given. The equivalent reform for Nigeria is not proposed as primary legislation, which would require action by the National Assembly on a longer and less certain timeline. It should instead be issued as an NDPC regulatory directive amending the GAID, using the Commission's existing power under Article 50 of the GAID to issue supplementary regulations and directives. A directive is preferable to an industry code because Article 50 already gives the NDPC unilateral power to amend the GAID. The directive should require that any cookie or tracking consent interface present "Accept" and "Reject" options with equal visual prominence, and should close the gap between Article 19(5) and Article 17(8)(b) by specifying that closing a privacy notice constitutes consent only to processing strictly necessary for basic website functionality, never to advertising, analytics, or personalisation cookies.
3. **Privacy Dashboards:** E-commerce platforms should be required to implement user-friendly privacy dashboards. This is to enable consumers to understand specific data permissions (e.g., opting out of third-party marketing while maintaining account functionality) without the threat of account deactivation.
4. **Defined Retention Periods:** Section 24 of the NDPA establishes storage limitation as a principle, requiring that data be retained no longer than necessary for the purpose collected; it does not itself specify a fixed retention period, and Article 49(3) of the GAID supplies only a general six-month default where no other time-bound obligation exists. The recommendation that platforms state exact retention periods by data category is accordingly a policy reform beyond what Section 24 currently requires, not a restatement of existing law. The most direct route for implementing it is to amend the NDP Act Compliance Audit Returns template (Schedule 2 of the GAID, filed annually under Article 10) to require a data controller to disclose its retention period for each category of personal data it processes, converting an internal audit obligation already in place into a public-facing disclosure requirement.
5. **Public Awareness:** The NDPC carried out the Digital Privacy Awareness Campaign (DPAC) in 2026.[63] The campaign targets young Nigerians in tertiary institutions; however, it is important to move this initiative beyond academic circles. NDPC can

[63] NDPC 'Catching Them Young: NDPC Takes 7th Digital Privacy Awareness Campaign to Ahmadu Bello University' < https://ndpc.gov.ng/catching-them-young-ndpc-takes-7th-digital-privacy-awareness-campaign-to-ahmadu-bello-university/accessed 2 September 2026

PRINT ISSN: 0794-0254

ONLINE: E-ISSN: 0794-084X

emphasize understanding data as a personal asset with enforceable legal rights. This will ensure that consumers are not only aware of their rights but are also actively engaged in ensuring their safety online. This will also ensure that they are equipped to report violations and demand accountability from e-commerce platforms.