CHAPTER 4

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

by

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

Osuolale, Olatunde Misbaudeen
Fountain University, Osogbo

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

Abstract

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

Introduction

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

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

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

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

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

Problem Statement

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

Literature Review

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

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

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

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

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

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

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

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

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

Materials and Methods

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

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

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

Discussion of Findings

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

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

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

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

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

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

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

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

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

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

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

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

Meta challenged the fine's procedural basis, claiming it was not given adequate notice. In April 2025, the Competition and Consumer Protection Tribunal upheld most of the decision but nullified one order due to due process concerns.[17,19] The company also challenged the proportionality of the fine, asserting that it exceeded the statutory limit tied to its Nigerian revenue. In its ruling, the tribunal upheld the penalty by referencing the seriousness and cross-border impact of the violation, as well as Meta's capacity to comply with data protection obligations. Nigerian law, however, bases penalties on domestic turnover and specified statutory maximums under Sections 48(4-6) and 49(1) of the Nigeria Data Protection Act, 2023, which limit fines to the

greater of ₦10 million or 2 percent of a data controller's or processor's annual gross revenue in Nigeria. This framework contrasts with the EU's GDPR, which expressly allows penalties calculated from global turnover.[20] Finally, fragmented oversight among the FCCPC, NDPC, NITDA, and ARCON continues to undermine regulatory coherence. Experts recommend a unified digital governance framework to improve coordination and enforcement.[21]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Policy Recommendations

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

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

Conclusion

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

References

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