

Social Media Platforms and the Commercialisation of Personal Data:

Evaluating Nigeria's Regulatory Responses



Introduction

Social media platforms' widespread collection and use of personal information have sparked concerns about users' privacy, personal freedoms, and the effectiveness of Nigeria's data protection framework.

Accordingly, this article argues that while the Nigeria Data Protection Act 2023 (NDP Act) is an important step toward regulating how personal data is collected, processed, and used commercially, significant challenges remain. It examines limited enforcement capacity, cross-border data transfers, and the difficulty of relying on user consent, and proposes measures to strengthen personal data protection.¹

2023

NDP ACT

An important step toward regulating how personal data is collected, processed, and used commercially — **yet significant challenges remain.**

Understanding the commercialisation of personal data

Commercialisation of personal data involves using information collected from individuals to create economic value through services, products and markets tailored to user preferences. Platforms derive substantial value from that data, while users receive only services whose benefits are often far outweighed by the value of the data collected.²

The commercialisation of personal data is facilitated through a variety of interconnected channels, where data may be obtained directly through online registrations, mobile applications, and social media platforms, and indirectly through tracking technologies such as cookies and web beacons, thereby enabling organisations to collect, process, and monetise personal information.³

While commercialisation has driven innovation and economic growth, it also raises ethical and legal concerns about how personal information is used.

How personal data is commercialised

DIRECT

Online registrations · Mobile applications · Social media platforms

INDIRECT

Tracking technologies — cookies · web beacons



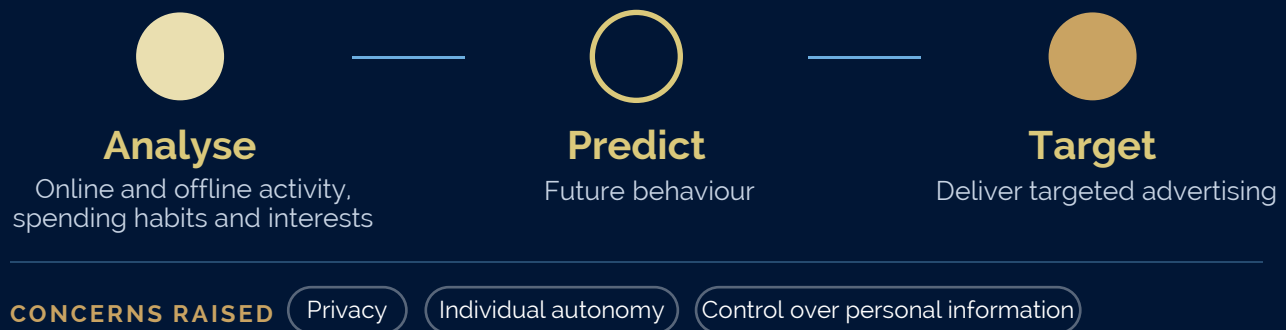
The Dark Side of Data Commercialisation

Much global commercial activity takes place on the internet.⁴ After individuals provide information online to access products and services, organisations often analyse and repurpose it beyond what users expect, creating a disconnect between what users expect and how organisations actually use their data.⁵

Personal data is increasingly treated as a commercial asset rather than an extension of identity, enabling organisations to track behaviour in ways individuals least expect.⁶ Sensitive personal data is particularly vulnerable to misuse, which may lead to identity theft, financial loss, or reputational harm.

Behavioural profiling is one of the most significant risks. Platforms analyse online and offline activity, spending habits, and interests; predict future behaviour; and deliver targeted advertising. Such practices improve commercial efficiency but raise concerns about privacy and individual autonomy.⁷ and the extent to which people control their personal information.⁸

How behavioural profiling works



Nigeria's Regulatory Response to Data Commercialisation

Nigeria's regulatory response to data commercialisation is grounded in the Constitution⁹ which guarantees the right to privacy and provides the constitutional foundation for subsequent data protection legislation. The NDP Act largely models itself on the European Union's General Data Protection Regulation (GDPR); however, the Nigerian Data Protection Act 2023 and General Application and Implementation Directive 2025 (GAID) reflect Nigeria's regulatory approach to social media data commercialisation.

The NDP Act requires controllers to conduct a Data Protection Impact Assessment (DPIA) before high-risk processing.¹⁰ The GAID identifies specific categories of data processing that require a mandatory DPIA, including certain cross-border data transfers and the use of CCTV surveillance in public places.¹¹ The GAID also requires mandatory DPIAs for specified high-risk processing activities and requires filing them with the NDPC. This adds a regulatory safeguard by requiring organisations to assess and mitigate privacy risks before implementing certain high-risk processing activities.¹²

The NDP Act adopts six lawful bases for processing,¹³ including legitimate interest reflecting Article 6(1) of the GDPR. Platforms generally wish to analyse user behaviour, personalise content or deliver targeted advertising without obtaining consent for every processing activity. However, a commercial interest alone does not establish a legitimate interest. The platform must demonstrate that the processing is within users' reasonable expectations and does not override their fundamental rights, freedoms and interests.¹⁴

The NDP Act also adopts the GDPR's right to data portability.¹⁵ For platforms where user data also drives market power, the right to portability has a competitive dimension. As social media platforms amass extensive datasets, they gain significant market influence; in response, the NDP Act empowers users to leave a platform with their personal data. Data portability lets users obtain and transfer their personal data to another platform, potentially lowering switching barriers and increasing user control over their data.¹⁶ However, portability does not prevent the original platform from retaining or continuing to process the data where it has a lawful basis to do so. This right would be enhanced if the NDP Act required data to be provided in interoperable, machine-readable formats, thereby facilitating meaningful transfers between platforms and reducing barriers to switching.¹⁷

The DPIA safeguard



GAID examples: certain cross-border data transfers · CCTV surveillance in public places

In addition, Nigerian courts are awarding damages against non-consensual commercial data use. In *Chukwunweike Akosa Araka v. Ecart Internet Services Limited & Eat 'N' Go Limited*,¹⁸ the Federal High Court awarded ₦3 million in damages for unsolicited direct marketing, ruling that repurposing customer details without explicit opt-in consent violates privacy rights. The decision sent a strong signal that Nigeria intends to hold companies accountable for breaches of its data protection laws.

Damages awarded

₦3m

Federal High Court · unsolicited
direct marketing

Chukwunweike Akosa Araka v. Ecart Internet Services Limited & Eat 'N' Go Limited

"A strong signal that Nigeria intends to hold companies
accountable for breaches of its data protection laws."

Where the Framework Faces Its Greatest Challenges

Enforcement Capacity

The NDPC operates in a vast, highly technical, and constantly evolving data ecosystem, and regulators with greater resources have struggled to monitor it comprehensively.

Data subjects face greater risk from the large-scale collection, profiling, and commercial exploitation of personal data underpinning many platform business models. Substantial financial penalties are unlikely on their own to change the behaviour of companies whose profitability depends on the commercial use of user data. Therefore, effectiveness will depend on sustained investment in the NDPC's capacity, technical expertise and enforcement tools.

CHALLENGE

Enforcement Capacity

Limited enforcement capacity

CHALLENGE

Cross-Border Data Transfers

CHALLENGE

Consent Fatigue

The difficulty of relying on user consent

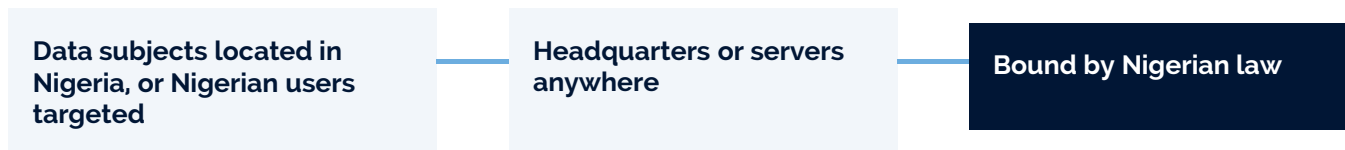
Cross-Border Data Transfers

Nigerians' personal data is routinely transferred to servers in other jurisdictions, often by organisations with no presence in Nigeria and limited familiarity with their obligations under Nigerian law.

The law curbs this with provisions establishing extraterritorial reach,¹⁹ and requiring any entity processing the data of subjects located in Nigeria, or targeting Nigerian users, to be bound by Nigerian law regardless of where its headquarters or servers reside.

Nigeria also regulates transfers of personal data outside the country through a comprehensive legal framework that permits them only when specific legal requirements, including adequacy determinations and recognised cross-border transfer instruments, are met.²⁰ Although data protection legislation has expanded significantly across Africa, regulatory gaps and differences in the scope, implementation and enforcement of national data protection frameworks persist.

Extraterritorial reach of Nigerian law



As of January 2026, 43 African countries had enacted data protection laws,²¹ although legislation does not necessarily guarantee effective enforcement or regulatory consistency. These disparities may create opportunities for regulatory arbitrage, whereby organisations seek to process or route personal data through jurisdictions with less stringent regulatory requirements. Against this backdrop, the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol provides a continental framework for addressing cross-border data governance. Its provisions on cross-border data transfers support efforts to facilitate digital trade while addressing differences in national regulatory approaches, and they are an important step toward regional harmonisation and an integrated African Digital Single Market. However, its effectiveness will depend on member states adopting it.

43

AS OF JANUARY 2026

African countries had enacted data protection laws.

Legislation does not necessarily guarantee effective enforcement or regulatory consistency — **opening room for regulatory arbitrage.**

Consent Fatigue

Consent as a safeguard against the commercialisation of personal data is particularly challenging in the Nigerian social media context, where lengthy privacy policies and standard-form terms may lead users to consent without fully understanding the extent of processing.²²

The NDP Act introduces safeguards by requiring consent to be freely and intentionally given, placing the burden on the controller to prove consent, and excluding silence or inactivity as valid consent.²³ It also prohibits conditioning access to a service on consent to processing that is unnecessary for the service. The GAID further requires sufficient information for informed consent and allows consent to be withdrawn as easily as it was given.

However, Nigerian jurisprudence has yet to develop the validity of digital or click-wrap consent. In *Chukwunweike Akosa Araka v Ecart Internet Services Nigeria Ltd & Eat 'N' Go Ltd*,²⁴ the Federal High Court considered consent in the context of direct marketing. However, it did not establish a general test for determining when accepting online terms constitutes valid data-protection consent. This leaves social media platforms that rely on click-wrap interfaces to obtain consent for extensive commercial processing uncertain.

The unresolved question

When does accepting online terms constitute valid data-protection consent?

No general test yet exists for digital or click-wrap consent — leaving platforms that rely on click-wrap interfaces uncertain.

Recommendations for Strengthening Data Protection in Nigeria

REGULATION

High-risk processing & click-wrap consent

Nigeria should strengthen regulation of high-risk processing, particularly profiling, targeted advertising and sensitive data processing. Clearer rules on click-wrap consent are also needed to ensure that digital consent is informed and valid.

CAPACITY

NDPC enforcement capacity

The NDPC's enforcement capacity should be enhanced through greater technical expertise, resources and collaboration with domestic and international regulators. This would improve monitoring and help address cross-border regulatory arbitrage

INTEROPERABILITY

Platform interoperability & portability

Finally, greater interoperability between digital platforms should complement the data portability right under the Nigeria Data Protection Act 2023 (NDP Act), enabling users to transfer their personal data more easily between service providers, reduce switching barriers and exercise greater control over their personal data.

Conclusion

Personal data has become one of the world's most valuable commercial assets, and social media platforms have built highly profitable business models around its collection and use. As the digital economy evolves, data protection regulation should evolve alongside it by providing stronger protection against high-risk processing, ensuring greater openness around algorithmic decisions, and continuing to build the NDPC's capacity to supervise and enforce compliance.

Contributors



Okechukwu Ekweanya

Partner, Data Protection



**Adedola
Adetokunbo-Ajayi**

Associate, Data Protection



Amarachi Juliet Nwosu

Associate, Data Protection

For further information on the issues discussed in this article,
contact our legal team at counsel@kennalp.com

Endnotes

1. Aprilia Dwi Santoso Putri and Rina Arum Prasastyanti, Personal Data Privacy in Social Media Platform: Governance, Ethics and Regulatory Measures, West Science Law and Human Rights Vol 3, No. 03, pp. 286-291.
2. Malgieri, G and Custers, B, 'Pricing Privacy – The Right to Know the Value of Your Personal Data' (2018) 34(2) Computer Law & Security Review 289–303. <https://doi.org/10.1016/j.clsr.2017.08.006>
3. <https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information>
4. UNCTAD, Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future (United Nations 2024) 12
5. Daniel J Solove, Understanding Privacy (Harvard University Press 2008) 98–120
6. Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books 2019) 199–223
7. Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books 2019) 291–327.
8. Anna Barker, "Organisation for Economic Co-operation and Development (OECD Roundtables on Competition Policy Papers No 247, OECD Publishing 2020)" 18–23
9. Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37
10. Nigeria Data Protection Act 2023, s 28(1)
11. General Application and Implementation Directive 2025 art 28(3)(k)
12. General Application and Implementation Directive 2025 Art 28(2)-(3)
13. Nigeria Data Protection Act 2023, s25
14. Nigeria Data Protection Act 2023, s 25(2)(a), (c)
15. Nigeria Data Protection Act 2023, s34, Regulation (EU) 2016/679 (General Data Protection Regulation) art 20.
16. Nigeria Data Protection Act 2023, s 38(2)(a)–(c)
17. Daniel Rubinfeld, 'Data portability and interoperability: An E.U.-U.S. comparison' (2024) 57 European Journal of Law and Economics 16
18. FHC/ABJ/CS/195/2024, Federal High Court, Abuja, 18 February 2025
19. Nigeria Data Protection Act (NDP Act) 2023, s 2, and the General Application and Implementation Directive (GAID) 2025, art 8
20. Nigeria Data Protection Act 2023, s 41–43; General Application and Implementation Directive 2025, art 45.
21. Nixon Kanal, "45 African Countries Have Enacted Data Protection Legislation" (Africa Business Communities, April 23, 2026) < <https://africabusinesscommunities.com/tech-24/45-african-countries-have-enacted-data-protection-legislation-yellow-card/> > accessed 16 October 2026.
22. Damiari, T. (2021), "Data Protection: WhatsApp Privacy Policy Changes and the Primacy of Consent Under Nigeria Data Protection Regulatory Framework", Nigerian Bar Journal, 11(2), 1-16.
23. Nigeria Data Protection Act 2023, s26(1) – (3)
24. supra



CONTACT

LAGOS

Kenna Place
8, Ogunyemi Road, Palace
Way, Oniru PO Box 73002,
Victoria Island,
Lagos

ABUJA

1st Floor, Novare Central,
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285,
Abuja

ENUGU

Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner, 400211
Enugu State.

+234 811 395 1052, +234 811 395 1053 | counsel@kennalp.com | www.kennalp.com