

When Consent Cannot Bear the weight: Artificial Intelligence, Algorithmic POWER and the Limits of Data Privacy Self-Management in Nigeria

Sam-Ibrahim, Folasade Emmanuella^{*1} Dr. Sodangi, Fadila Abubakar²

¹LLB (Kogi State University, Anyigba); LLM (University of Ibadan); PhD Candidate, Nile University of Nigeria. Email: arasamibrahim@gmail.com

²Associate Professor, Lecturer, Faculty of Law, Nile University of Nigeria, Email: fsodangi.abubakar@nileuniversity.edu.ng

Abstract

Nigeria's data protection laws rely on a borrowed foundation. The Nigeria Data Protection Act 2023, like the regulation it replaced, treats the individual's consent as the moral and legal centre of gravity of lawful processing, reiterating the control-based conception of privacy that Nigerian courts have read into section 37 of the Constitution. This article argues that artificial intelligence has undermined that foundation. Machine learning systems derive their value from processing that individuals cannot foresee, inspect, or meaningfully refuse: large-scale inference, profiling that outruns any disclosed purpose, the repurposing of ordinary data as training material, and the fusion of biometric identity infrastructures whose consequences cannot be withdrawn. Drawing on Nigeria's own experience, including the compulsory linkage of the National Identity Number to mobile SIM cards, the opening of the national biometric database to security agencies, and the punitive analytics of digital lenders, the article shows that consent in the age of artificial intelligence functions less as a safeguard than as a ritual of authorisation that transfers risk to the very people it purports to protect. It contends that reform should shift the centre of gravity of Nigerian privacy law from individual control towards institutional accountability and data justice: enforceable purpose limitation, mandatory algorithmic impact assessment built on the Act's existing machinery, genuine constraints on solely automated decisions, and collective avenues of redress. Privacy, so understood, is not a private preference to be waived but a public safeguard on algorithmic power.

Keywords: artificial intelligence; data privacy; consent; algorithmic accountability; Nigeria Data Protection Act 2023; data justice

INTRODUCTION

Every serious data protection regime must answer a deceptively simple question: under whose authority may one person process another person's personal information? Nigeria, like most jurisdictions that have legislated in the long shadow of the European Union's General Data Protection Regulation, has answered by placing the individual's consent at the centre of the enquiry. The Nigeria Data Protection Act 2023 ("the Act") makes consent the first and most conspicuous lawful basis for processing, and it surrounds that consent with the now-familiar guarantees that it must be freely given, specific, informed and unambiguous, and signalled by a clear affirmative act rather than inferred from silence or inactivity. Beneath the statutory text lies a deeper commitment. The Act's structure is built on the idea that privacy depends fundamentally on individual control. So long as an individual is well informed and consents, their privacy is considered safeguarded. Nigerian courts have written this assumption into constitutional law, interpreting the right to privacy under section 37 of the Constitution as encompassing an individual's control over the flow of information about them.

This article argues that artificial intelligence has quietly rendered that assumption untenable and that Nigerian law has not yet caught up. The control model was strained long before machine learning arrived; scholars have warned for over a decade that the burden it places on the individual is unrealistic. Artificial intelligence converts that strain into structural failure. The systems now being deployed in Nigeria in identity management, financial services, telecommunications and policing derive their value precisely from operations that the data subject cannot anticipate at the moment of collection, cannot inspect once they are running, and cannot decline without forfeiting participation in economic and civic life. Where that is the case, consent does not constitute a meaningful choice. It

describes a signature on a form.

The argument proceeds in six steps. Part 2 reconstructs the inheritance: the conception of privacy as control, its constitutional expression in Nigeria, and the passage of that conception from the Nigeria Data Protection Regulation 2019 into the Act of 2023. Part 3 sets out four structural reasons why artificial intelligence defeats consent as a protective device. Part 4 tests the argument against Nigerian practice, drawing on the National Identity Number-SIM linkage, the exposure of the biometric database to security agencies, and the conduct of digital lenders. Part 5 advances the constructive claim: that Nigerian reform should shift its centre of gravity from individual control to institutional accountability and data justice, and that the materials for that shift already lie within the Act. Part 6 answers the obvious objections. The case is offered not as a parochial complaint but as a study of a wider predicament: what happens when a consent-centred model borrowed from Europe meets the extractive data practices of a rapidly digitising state in the Global South.

2. The Inheritance: Privacy as Control and Consent as Its Instrument

The idea that privacy is a form of control over personal information is among the most durable in the field. Alan Westin's formulation of privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others has shaped statutes, regulations and constitutions over five decades. Its attraction is obvious. Control speaks the language of autonomy and dignity; it casts the data subject as an agent rather than an object; and it supplies regulators with a tidy operational vocabulary. If privacy is control, then a regime protects privacy by securing the individual's consent and by policing the terms on which that consent is obtained. Daniel Solove has named the resulting model "privacy self-management": the law gives every individual the right to manage the level of access they grant and to revise it at any time.

Nigerian law has absorbed this conception at both constitutional and statutory levels. Section 37 of the Constitution guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. The provision is terse, and for many years its reach was uncertain; the Court of Appeal read it narrowly in some contexts and expansively in others. The decisive turn came in *Digital Rights Lawyers Initiative v NIMC*, where the Court of Appeal held that the fundamental right to privacy in section 37 encompasses the protection of personal data. Data protection in Nigeria is therefore not merely a creature of regulation; it is a constitutional right, and it inherits the fundamental status of constitutional law.

The Nigeria Data Protection Regulation 2019, issued by the National Information Technology Development Agency, imported the wording of the General Data Protection Regulation almost verbatim and made consent its bedrock. The Act of 2023, which repealed the Regulation, established the Nigeria Data Protection Commission as a dedicated supervisory authority and was in turn supplemented in 2025 by the Commission's General Application and Implementation Directive (GAID). Although the core concept was preserved, the Act sets out six lawful bases for processing: consent, contractual necessity, legal obligation, vital interests, public interest or official authority, and legitimate interests, but consent remains the presumptive gateway, the basis on which data controllers most readily proceed. Consent must be affirmative and specific; it may be withdrawn; and it cannot be manufactured from pre-ticked boxes.

Why did the Nigerian legislature adopt this model so readily? The answer lies largely in the desire to align with global trends. Alignment with the GDPR paves the way for an adequacy determination, making cross-border data flows seamless; a consent-centred statute that mirrors European standards signals to investors and partners that Nigerian law meets a recognised international benchmark. Consent is also administratively convenient: it converts a hard question about the legitimacy of processing into a procedural one about whether a form was completed, and it spares the regulator the harder task of determining how far the data obtained may lawfully be used. The result, however, is that Nigeria imported not only the strengths of the European model but also its central vulnerability: a near-total dependence on individual consent at a moment of rapid and largely ungoverned digitisation.

None of these rationales is objectionable in itself. The difficulty is that the model Nigeria adopted was already

showing its age even at the time of adoption. The critique of “notice and choice” is by now familiar: privacy policies are unread and unreadable; the aggregate cost of managing one’s data across every service is impossibly high; and consent, once given, tends to authorise far more than the data subject imagined. Richards and Hartzog articulate the point with precision in their cataloguing of digital consent pathologies, unwitting, coerced and incapacitated assent that nonetheless retains legal validity. These problems already existed in a world of databases and mailing lists. Artificial intelligence makes them fatal.

3. Why Artificial Intelligence Breaks Consent

Four features of machine learning, taken together, dismantle consent as a protective device. Each maps onto a requirement the Act sets for valid consent, and each shows that, in the context of artificial intelligence, meeting that requirement is almost impossible in practice.

3.1 The Collapse of the “Informed” Requirement: Scale and Opacity

Consent must be informed, which presupposes that the data subject can understand what they are agreeing to. Machine learning defeats that presupposition twice over. First, the sheer scale of modern processing the number of controllers, purposes and data flows implicated by an ordinary act of digital participation exceeds any individual’s capacity to attend to it. Second, and more fundamentally, the systems themselves are opaque. A model’s behaviour emerges from the statistical interaction of millions of parameters; even its designers cannot predict its output. Frank Pasquale’s image of the “black box” captures the asymmetry precisely: those who are scored, sorted and judged by algorithmic systems are denied the very information needed to evaluate the bargain. Consent to a process one cannot inspect is not informed consent; it is deference dressed as agreement.

3.2 The Collapse of the “Specific” Requirement: Inference and Purpose Creep

Consent must be specific, tied to defined purposes disclosed at the point of collection. Artificial intelligence is, by design, an engine for exceeding disclosed purposes. Its distinctive power lies in the inference, the derivation of new and often sensitive information from seemingly innocuous data. From a pattern of transactions, a model infers health status; from location traces, it infers religion or political affiliation, and, in some cases, emotional state. None of this inferred knowledge was disclosed at collection, because none of it existed at collection; the system manufactures it. The “specific purpose” to which the data subject consented thus becomes a point of departure rather than a limit. Helen Nissenbaum’s theory of contextual integrity explains why this feels like a violation even where a literal reading of the consent form permits it: information collected in one context, governed by one set of norms, is transposed into another where those norms do not hold. While the Act’s principles of purpose limitation and data minimisation acknowledge the danger, consent once obtained is too often treated as the mechanism that overrides them.

3.3 The Collapse of the “Freely Given” Requirement at the Point of Secondary Use

Consent must be freely given, and it must attach to a purpose. Yet the value of personal data to artificial intelligence lies overwhelmingly in secondary use in the repurposing of data collected for one end as training material for models serving quite another. The photograph uploaded to verify identity trains a facial recognition system; the call records retained for billing feed a fraud-detection model; the loan repayment history becomes a variable in a credit-scoring algorithm sold to third parties. Shoshana Zuboff’s account of surveillance capitalism describes this as the extraction of a “behavioural surplus” whose downstream uses are, by commercial necessity, kept from the person who generated it. Consent obtained at collection cannot be free with respect to uses that had not been conceived when it was given. The data subject is not choosing; she is being enrolled in a future she cannot see.

3.4 The Collapse of Individual Remedy: Aggregation and Irreversibility

Finally, consent is an individual act, assuming the harm it prevents is personal and reversible. However, artificial intelligence causes damages that are often collective and irreversible. Its injuries often affect groups, for example, a discriminatory model harming a class of people, not just the individual claimant. When biometric data is involved, these harms tend to be irreversible. A password can be changed; a face, a fingerprint or an iris cannot. Once such

data is enrolled and linked across systems, no subsequent withdrawal of consent can restore the prior state of the world. Nick Couldry and Ulises Mejias argue that this large-scale appropriation of human life as data reproduces the logic of colonial extraction, converting the substance of social existence into a resource for others' profit and control. Their framing is deliberately provocative, but it identifies something the consent model cannot see: that the stakes are structural, concerning the distribution of power between institutions and populations, rather than the preferences of discrete individuals. As Julie Cohen observes, privacy is not only a private good but a public one, the breathing room a self-governing society needs to form citizens capable of resisting the pull of surveillance. A regime that treats privacy as a waivable personal preference cannot protect that public interest, because it permits the interest to be signed away one click at a time.

Taken singly, each of these failures might be met with a patch, clearer notices, tighter purpose statements, shorter retention. Taken together, they describe a paradigm that no amount of patching can rescue, because the difficulty is not that consent is badly implemented but that the object to which it is meant to attach has changed. Solove's deeper point about aggregation applies with full force: a series of individually trivial disclosures, each rationally consented to, combines into a portrait of a person that none of the individual consents contemplated or authorised. Artificial intelligence is the aggregation engine par excellence. A regime that assesses the legitimacy of processing one consent at a time will always be blind to the harm that lives in the combination, and it is the combination that artificial intelligence is built to exploit.

4. The Nigerian Evidence: Consent as Ritual

These are not abstract anxieties. Nigeria's recent digital history furnishes a set of vivid illustrations, each showing consent operating not as a safeguard but as a ritual of authorisation. This formality launders coercion or surveillance into apparent agreement.

4.1 The National Identity Number-SIM Linkage

From 2020, the Federal Government required every mobile subscriber to link their National Identity Number to their SIM card, with disconnection as the penalty for non-compliance. Verification was to proceed by biometric means, fingerprints and facial recognition matched against the database held by the National Identity Management Commission. The policy was voluntary in form and compulsory in substance: a person was free to withhold her biometric identity only at the price of exclusion from the mobile network that now mediates banking, employment and access to government itself. To call the resulting enrolment "consensual" is to empty the word of content. The choice on offer surrender your biometrics or be cut off is precisely the coerced choice that the Act's "freely given" standard is meant to forbid, yet it was imposed at a national scale on tens of millions of people.

4.2 Function Creep and the Biometric Database

The irreversibility problem then materialised. In 2022, it emerged that the President had approved security agencies' access to the National Identity Management Commission's database via the very linkage infrastructure that citizens had been compelled to feed. Civil society organisations protested that the arrangement lacked any basis in legality, necessity or proportionality, and warned that millions of law-abiding Nigerians might reasonably feel themselves under constant surveillance. The episode is a textbook instance of function creep: data gathered for identity verification, on one stated purpose, was made available for an entirely different one, without fresh consent and without meaningful oversight. The enabling conditions were structural. The National Identity Management Commission Act permits disclosure of database information without an individual's consent in the interest of national security, and the 2023 Act exempts processing for national security and crime prevention from significant parts of its scheme. Consent, in this domain, is not merely inadequate; it is legally beside the point.

4.3 Algorithmic Lending and the Private Sector

The private sector supplies the mirror image. Nigeria's digital lending market runs on algorithmic credit scoring built from data harvested through mobile applications, contact lists, call logs, device identifiers and transaction histories. Borrowers routinely grant sweeping permissions to obtain small, short-term loans, only to find, on default, that the

same data is turned against them: automated systems dispatch defamatory messages to the contacts scraped from their phones, a practice that Nigerian courts have begun to recognise as a violation of the right to privacy. Here, consent is not coerced by the state but buried in permissions that no borrower reads, and none can negotiate. The pattern echoes the Court of Appeal's earlier condemnation, in *Emerging Markets Telecommunication Services Ltd v Eneye*, of disclosing a subscriber's number for unsolicited messaging as an infringement of section 37. What has changed is that the disclosure is now automated, industrialised and lucrative, and the "consent" that authorises it is manufactured at the point of installation.

The lending market does not operate in isolation. It sits atop a financial identity infrastructure, the Bank Verification Number, itself a biometric identifier introduced by the Central Bank. That already binds a person's transactions, devices and contacts into a single traceable profile. Layered onto that infrastructure, algorithmic scoring does not merely assess an applicant; it aggregates and repurposes a life. The borrower who "consents" to a loan application is, in substance, consenting to the fusion of data she has surrendered across a dozen unrelated encounters, for uses she was never shown. This is the aggregation problem in commercial dress, and it is spreading through the very sector that Nigeria most wishes to grow.

4.4 A Recognised Right without a Working Remedy

Against these deployments, the protective apparatus remains thin. The constitutional right is now settled, but its enforcement is nascent: the reported jurisprudence recognises the right far more confidently than it fashions remedies for its breach, and the volume of litigation remains small relative to the scale of processing. The Nigeria Data Protection Commission is young, and although the General Application and Implementation Directive of 2025 has begun to supply the operational detail that the Act left open, the Commission's capacity to audit, investigate and sanction algorithmic systems at scale remains unproven. The cumulative picture is of a regime that has recognised privacy as a right, equipped it with a consent-centred toolkit, and then watched that toolkit fail to constrain the very deployments that most threaten the right. Across the public and private examples alike, consent performs a single consistent function: it transfers risk from the institution that processes to the person whose life is processed.

5. Beyond Control: Accountability and Data Justice

If consent cannot bear the weight, what should? The answer is not to abolish consent but to demote it to remove it from the load-bearing position it currently occupies and to build the regime's protective strength elsewhere. The organising idea is accountability: the allocation of responsibility to the institutions that design and deploy data systems, enforced independently of whether any individual has agreed to anything. Four reforms would give that idea effect in Nigeria, and each can be constructed from materials already present in the Act.

5.1 Purpose Limitation and Design Obligations as Enforceable Duties

The Act already states the principles of purpose limitation, data minimisation and integrity. Currently, these operate largely as background norms, easily displaced by a broadly drafted consent. They should instead be treated as substantive, non-waivable duties owed by controllers, breach of which grounds liability regardless of consent. The burden of justifying a processing operation of showing that it is necessary, proportionate and confined to its stated purpose belongs on the institution that profits from it, not on the individual who cannot see it. Consent obtained at collection should not license the later repurposing of data as training material unless that repurposing independently satisfies the principles. This single move would neutralise the secondary-use problem that artificial intelligence exploits.

5.2 Algorithmic Impact Assessment Built on the Act's Existing Machinery

Section 28 of the Act requires a data privacy impact assessment when processing is likely to pose a high risk to data subjects' rights and freedoms. This provision is the natural anchor for a mandatory algorithmic impact assessment regime. For high-risk deployments of biometric identity systems, automated credit scoring, and algorithmic policing, the assessment should be obligatory, address discriminatory and collective effects rather than security alone, and, in the case of public-sector systems, be published and subject to the Commission's review before deployment.

Impact assessment shifts scrutiny to the design stage, where harms can still be prevented, and it does so without asking the data subject to understand a system that its own engineers may struggle to explain.

5.3 Genuine Constraints on Solely Automated Decisions

Section 37 of the Act confers a right not to be subject to a decision based solely on automated processing where that decision produces legal or similarly significant effects. On paper, this mirrors the European position; in practice, it risks becoming a dead letter, easily evaded by the token inclusion of human involvement. The right requires teeth: a genuine entitlement to human review by a person with authority to reach a different conclusion, to an explanation of the basis of the decision, and to contest it. In the highest-stakes contexts, above all, the presumption should be reversed; solely automated determination should be prohibited rather than merely resistible. A right that the data subject must invoke, against an institution she cannot see and cannot match, is no protection at all.

5.4 Collective Redress and a Data-Justice Lens

Because algorithmic harms are frequently collective, the avenues of redress must be collective too. Nigeria's own experience points the way: it was public-interest litigation by civil society, not individual claims, that secured constitutional recognition of data protection in the first place. The law should build on that by equipping representative bodies with clear standing to bring actions on behalf of affected classes, and by recognising group harms discrimination, systemic surveillance as compensable in their own right. This reorientation is best understood through the lens of data justice, which connects data governance to broader questions of fairness, power and freedom rather than to individual control alone. For a jurisdiction in the Global South, the point is not to reproduce Europe's statute more faithfully but to protect Nigerians from asymmetries of informational power that a consent model, transplanted without adaptation, tends to entrench. African data protection scholarship has long cautioned against mistaking legislative mimicry for protection, and the caution is well taken here.

The data-justice frame does more than relabel existing rights. It reorients the questions the law asks. Instead of enquiring only whether a given individual agreed to a given processing operation, it asks who bears the risks and who reaps the rewards of a data system; whether particular groups are rendered disproportionately visible, or disproportionately misjudged, by its operation; and whether the population subjected to the system has any collective say in its design. These are questions a consent form cannot pose. For Nigeria, they are the right questions, because the systems that matter most national identity, financial scoring, telecommunications surveillance are precisely those whose effects are distributed across whole populations rather than borne by isolated individuals who might, in theory, have clicked "no."

5.5 Institutional Capacity as a Precondition

None of this will work without an institution equal to the task of enforcing it. The Commission must be adequately resourced, genuinely independent, and equipped with sanctions that are proportionate and sufficiently dissuasive to alter the conduct of well-capitalised controllers. Accountability is only as real as the institution that demands it; a duty no regulator can enforce is, from the data subject's vantage, indistinguishable from no duty at all. Reform of the substantive law and investment in the supervisory authority are therefore not alternatives but parts of a single programme.

6. Objections

Three objections deserve a direct answer. The first is that demoting consent is paternalistic, substituting the regulator's judgment for the individual's autonomy. But the argument is not that consent should disappear; it is that consent should be confined to the discrete, low-stakes, revocable choices it can actually govern, and relieved of duties it cannot. Preserving a hollow ritual of choice does not honour autonomy; it exploits its appearance. Genuine autonomy is better served by a regime that prevents harm than by one that secures a meaningless signature and calls the matter closed.

The second objection is economic: that accountability duties will burden a digital economy that Nigeria is anxious to grow. This mistakes the relationship between trust and growth. A digital economy in which citizens reasonably fear

that their biometric identities are surveilled and their data weaponised is not a flourishing one; trust is a precondition of participation, not a tax upon it. Moreover, the accountability model is calibrated to risk. It asks little of low-risk processing and much of the high-risk systems that pose the gravest threats, a proportionality that the blunt instrument of universal consent cannot achieve.

The third objection is that this reproduces the European apparatus of impact assessment and automated decision-making rights under another name. The resemblance is real, but the orientation is different. The proposal shifts the regime's centre of gravity from the individual to the institution, insists on enforcement realism rather than paper rights, and reads the whole through a data-justice lens attentive to the position of a Global South state importing both the technology and the law from elsewhere. That is not mimicry; it is adaptation, which is what the transplant needed in the first place.

7. Conclusion

Nigeria has built its data protection regime on the conviction that privacy is control and that consent is its instrument. That conviction was serviceable in the era of databases and defensible in the abstract. Artificial intelligence has overtaken it. The systems now reshaping Nigerian public and private life extract their value from processing that no data subject can foresee, inspect or refuse, and they do so most consequentially in the domain of biometric identity, where the harm can never be undone. In that setting, consent is not a safeguard but a mechanism for transferring risk to the governed. The National Identity Number-SIM linkage, the opening of the biometric database to security agencies, and the punitive analytics of digital lenders are not aberrations; they are what a consent-centred regime predictably permits.

The remedy is to shift the centre of gravity of Nigerian privacy law from individual control to institutional accountability and data justice, and to do so using the machinery the Act already contains: purpose limitation as an enforceable duty, algorithmic impact assessment grown from the existing data-privacy-impact provision, solely-automated-decision rights with genuine teeth, and collective redress before a Commission with the capacity to use it. On this account, privacy is not a private preference to be waived at the point of collection but a public safeguard on algorithmic power, a constraint that a self-governing society places on the institutions that would otherwise process its members without limit. Finding the balance between innovation and protection is the task of the coming decade, in Nigeria as elsewhere. It will not be found by asking individuals to consent to what they cannot understand.

Disclosure Statement on the Use of Artificial Intelligence

In preparing this article, the author used Grammarly and Claude (Anthropic). These tools were used for language editing, expression refinement, structural and stylistic revision of the manuscript, and assistance with formatting and organisation of the footnotes and bibliography. All research questions, arguments, analysis, interpretation and conclusions are the author's own. The author reviewed, verified and edited all AI-assisted output, including the accuracy, neutrality and completeness of every citation and reference, and accepts full responsibility for the content of the article.

References

1. Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press, 2006.
2. Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press, 2014.
3. Cate, Fred H. "The Failure of Fair Information Practice Principles." In *Consumer Protection in the Age of the Information Economy*, edited by Jane K. Winn, 341-377. Aldershot: Ashgate, 2006.
4. Cohen, Julie E. "What Privacy Is For." *Harvard Law Review* 126, no 7 (2013): 1904-1933.
5. Couldry, Nick, and Ulises A. Mejias. *The Costs of Connection: How Data Is Colonising Human Life and*

- Appropriating It for Capitalism. Stanford: Stanford University Press, 2019.
6. Couldry, Nick, and Ulises A. Mejias. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20, no 4 (2019): 336-349. <https://doi.org/10.1177/1527476418796632>.
 7. "Crystalite Solicitors. "Data Protection: Legal Remedy to Loan Apps Menace." October 22, 2024. <https://crystalitesolicitors.com/data-protection-legal-remedy-to-loan-apps-menace/>. Accessed July 2, 2026.
 8. Makulilo, Alex B., ed. *African Data Privacy Laws*. Cham: Springer, 2016.
 9. "Hersey, Frank. "Nigeria: Privacy Concerns Mount over Digital ID–SIM Link as Deadline Approaches." *Biometric Update*, August 6, 2021. <https://www.biometricupdate.com/202108/nigeria-privacy-concerns-mount-over-digital-id-sim-link-as-deadline-approaches>. Accessed July 7, 2026. Accessed 28 June 2026.
 10. Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.
 11. Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.
 12. Richards, Neil, and Woodrow Hartzog. "The Pathologies of Digital Consent." *Washington University Law Review* 96, no 6 (2019): 1461-1503.
 13. "Macdonald, Ayang. "Security Agencies Granted Access to Nigeria's Biometric Database; Buhari Faces Lawsuit." *Biometric Update*, March 15, 2022. <https://www.biometricupdate.com/202203/security-agencies-granted-access-to-nigerias-biometric-database-buhari-faces-lawsuit> accessed 27 June 2026.
 14. Socio-Economic Rights and Accountability Project (SERAP), Letter to President Muhammadu Buhari on Unlawful Access to Subscribers' Details via NIN-SIM Linkage, 5 February 2022, available at <https://serap-nigeria.org/2022/02/06/nin-sim-linkage-serap-writes-buhari-over-unlawful-access-to-subscribers-details/> accessed 2 July 2026.
 15. Solove, Daniel J. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126, no 7 (2013): 1880-1903.
 16. Taylor, Linnet. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society* 4, no 2 (2017): 1-14. <https://doi.org/10.1177/2053951717736335>.
 17. Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.
 18. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.
 19. Nigeria
 20. *Araka v Ecart Internet Services Nigeria Ltd* (2025) (Federal High Court).
 21. Constitution of the Federal Republic of Nigeria 1999.
 22. *Digital Rights Lawyers Initiative v National Identity Management Commission* (2021) LPELR-55623(CA).
 23. *Emerging Markets Telecommunication Services Ltd v Eneye* (2018) LPELR-46193(CA).
 24. National Identity Management Commission Act 2007.
 25. Nigeria Data Protection Act 2023.
 26. Nigeria Data Protection Commission, General Application and Implementation Directive 2025.
 27. Nigeria Data Protection Regulation 2019.
 28. *Nwali v Ebonyi State Independent Electoral Commission* (2014) LPELR-23614(CA).
 29. European Union
 30. General Data Protection Regulation (Regulation (EU) 2016/679).
 31. African Union
 32. African Union Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention).