Data Privacy Laws: Implications in the Tech Space
By Folarinwa Aluko

Every click, every scroll, every online interaction leaves behind a digital footprint — proof that in the age of algorithms, the internet never forgets. More than ever, data has become the lifeblood powering Nigeria's vibrant entertainment, fashion, and technology industries. But as artificial intelligence (AI) deepens its grip on how this data is collected and used, a pivotal question surfaces: What kind of legal framework do we truly need to protect our digital privacy — not just in theory, but in reality?

Privacy's Evolving Battleground: From Analogue to AI
For decades, privacy in Nigeria was defined by space and silence— the boundaries of a home, the confidentiality of letters, the discretion of phone calls, guaranteed by Section 37 of the 1999 Constitution which safeguards "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications."
In that analogue world, data was physical, finite, and easier to control. Breaches were localized and traceable. But the digital shift rewrote the rules.

The emergence of the internet — and now AI — has transformed data into something ambient, infinite, and often invisible. Early legislative responses like the Nigeria Data Protection Regulation (NDPR) 2019 offered a foundational start, but as a subsidiary regulation, its legal weight was limited. The Nigeria Data Protection Act (NDPA) 2023 promised a bolder, more comprehensive stance.
Yet beneath its surface lie foundational questions: Is it built on constitutional certainty? And does it do enough to address the complex, often subtle ways data is harvested and manipulated today?

Building on Solid Ground: The Constitutional Imperative
A future-facing digital privacy regime must rest on solid legal bedrock. Yet, a core Constitutional question persists: Is privacy a federal concern, or a residual matter left to Nigeria's 36 states?

Because "Privacy" is not expressly mentioned in the Exclusive or Concurrent Legislative Lists, and since Section 4 of the Constitution reserves all residual matters to the states, one could argue that the burden of Privacy (read Data Protection) legislation sits with the States. If this interpretation prevails, the NDPA's authority could be challenged — potentially opening the door for a patchwork of state laws, each with its own standards, requirements, and enforcement strategies.

That legal uncertainty is a risk — not just for policymakers, but for businesses, developers, creators, and consumers. Nigeria must either constitutionally define data protection as a federal mandate or explicitly anchor its legitimacy through a clearly delegated legislative

instrument. Without such clarity, confidence in the system — and compliance with it — may falter.

Rethinking Regulation: Beyond Revenue

For any data protection framework to succeed, the regulatory philosophy must shift. It must evolve from one centered on fines and fees to one grounded in civic empowerment. The first question to answer is whether we need a new entire agency to 'regulate' data protection

If regulatory bodies are seen — or structured — primarily as revenue generators, the legitimacy of their mission suffers. The NDPC's publicized revenue targets, where the agency boasts to recoup money for government, are nothing short of scandalous and risk overshadowing its role as a rights guardian. This isn't just perception—it affects how laws are implemented and who ultimately pays.

Startups and small businesses already face steep compliance burdens. Annual registration fees, mandated audits, and impact assessments can throttle innovation at the grassroots. These costs trickle down to consumers, often without proportionate privacy gains.

This raises a deeper question: do we actually need a standalone Data Protection Commission? In a digital economy where data flows through every sector, why isolate regulation in a siloed agency? Could data governance not be more efficiently and democratically integrated into existing institutions—like the Consumer Protection Commission, sectoral regulators, or civil courts—via robust guidelines and enforceable rules? When data is everywhere, should its protection not be everywhere too?

Creating a new bureaucracy to manage something so foundational runs the risk of fragmentation, overlap, and inconsistent application—especially in a legal system already burdened with too many overlapping agencies. Instead of consolidating control, it may be more effective to decentralize responsibility but standardize rules, with public accountability mechanisms embedded across sectors.

True regulation should reward "privacy-by-design," offer support for SMEs, and focus on prevention, not just punishment. Empowering compliance isn't soft—it's strategic. This is especially important in the creative sector, where a recent IP & Entertainment Law Survey by the Intellectual Property Lawyers Association Nigeria (IPLAN) found that over 60% of creators had unknowingly consented to exploitative data practices buried in standard platform agreements.

What Privacy Laws Must Account For: The AI Conundrum

AI's ability to extract, interpret, and act on data — often without explicit consent — has fundamentally changed what privacy even means.

Consider your favorite streaming app or fashion store. You scroll. Pause. Linger. Without typing a word, AI has already begun decoding your preferences, inferring your mood, predicting your next desire. This is inferred data — insights you didn't knowingly give but which now define your experience.

That data may be used to manipulate: tailoring prices, suggesting products, or prompting impulse decisions based on your emotional state. The manipulation is subtle, the interface friendly, but the impact profound.

During a recent session at the Intellectual Property Lawyers Association Nigeria Clinic, we explored an interesting case where a Creator had been subjected to digital overreach by an exploitative platform. Our current legal focus on consent — those dense "terms and conditions" few ever read — is no longer enough. Nigeria's privacy law must mandate radical transparency in AI systems: explainable decisions, clear opt-outs, and enforceable rights to challenge automated profiling. Otherwise, we risk codifying a world where people are nudged without knowing, judged without hearing the evidence, and shaped by machines they cannot interrogate.

Privacy Is Power

Privacy is not a luxury. It's a right—one tied to dignity, autonomy, and freedom.

But rights only matter when they're usable. The average Nigerian — artist, trader, fashion designer, student — must be able to access, correct, and challenge how their data is used. Not through a costly court case. Not through a 20-page legal letter. But through clear, affordable, intuitive mechanisms: online portals, local ombudsman structures, and simplified dispute channels.

Conclusion

Nigeria stands at a pivotal threshold. The NDPA 2023 is a landmark effort, but legislation alone will not secure our digital future. We need more than codes and commissions — we need vision, clarity, and enforcement that is centered on People, not profits.

The goal isn't to create a fortress of regulation- that stifles creativity. It's to build a trusted digital commons, where rights are protected, innovation thrives, and AI serves human dignity—not corporate secrecy.

The journey toward meaningful privacy protection is just beginning. What we design today will shape not just data policy, but democracy itself.

Folarinwa Aluko is a Legal Practitioner and Partner in the firm of Trumann Rockwood Solicitors. He can be reached at fmaluko@trumann-rockwood.com