10TH ANNIVERSARY

LAWYARD®



SPECIAL EDITION

LAWYARD DATA PROTECTION AND PRIVACY JOURNAL



TOBI ADEWALE

FOUNDER, LAWYARD



LATE ALAO ADAVISE

CO-FOUNDER, LAWYARD



GBOLAHAN BADMUS

EDITOR-IN-CHIEF

PUBLISHER'S NOTE

Ten Years of Knowledge, Memory, and Purpose

Ten years ago, a dream that began at the Faculty of Law, Obafemi Awolowo University, took its first steps into the public sphere. Lawyard was born from a shared conviction — that knowledge should be accessible, that the law should serve people, and that young lawyers must have a voice in shaping the conversations that define their future. My late friend, Adavize Alao, embodied that conviction. His passion for technology, innovation, and the protection of human dignity continues to inspire every stride we take today.

This Special Privacy Edition of the Lawyard Journal is both a commemoration and a continuation of that vision. The Adavize Alao Essay Competition was in 2019 instituted in his honour to sustain thought leadership in privacy and data protection, an area of law that has grown from obscurity to urgency within a single decade. From our first essays on Nigeria's data protection framework in 2019 to the current debates on artificial intelligence and digital surveillance, this journal documents a generation of lawyers, students, and researchers who have taken up the challenge to define privacy for the digital age.

We are proud that since inception, nearly a thousand young legal minds have participated in this initiative, with past winners like Victoria Oloni, Gabriel Omoniyi, Mary Omobolanle, Imoter Kpengwa, Olufolajimi Otitoola, Ikenna Mba, Abdulganiy Olayinka, and Mujeebat Idris contributing to the growing archive of privacy scholarship in Nigeria and beyond. Their essays — and those before them, remind us that privacy is not merely a technical or regulatory concern, but a deeply human one, central to freedom, autonomy, and dignity.

As Lawyard celebrates its tenth anniversary, this edition is a testament to how far we have come and how much further we must go. It honours the life and ideals of Adavize Alao, while reaffirming our commitment to empowering the next generation of lawyers to think critically, act ethically, and build responsibly in a world increasingly shaped by technology.

To every contributor, partner, editor, and reader who has walked with us on this journey, we say 'thank you'. The story of Lawyard continues because you keep believing in the power of ideas.

Tobí Adébọ̀wálé
Founder / Team Lead, Lawyard
tobi@lawyard.org

EDITOR'S NOTE

Privacy, Innovation, and the Law: A Continuum of Reflection

Over the past decade, Lawyard has evolved from a digital legal community into a thought leader shaping conversations at the intersection of law, technology, and society. With each issue of the Lawyard Journal, we have sought to capture the rhythm of our time — how law responds to, and sometimes resists, the transformations that define our nation and our world.

This Special Privacy Edition continues that mission, but with a singular focus: to honour the memory of Adavize Alao and to chronicle, through the voices of our essay competition winners from 2019 to 2025, the evolution of privacy and data protection law in Nigeria.

The Adavize Alao Essay Competition on Privacy and Data Protection, founded in 2019, began as a modest effort to inspire young lawyers and students to engage with a then-emerging field. Six years later, it stands as one of Nigeria's most enduring platforms for intellectual exchange on privacy, data governance, and digital rights. From the earliest essays interrogating the adequacy of Nigeria's data protection frameworks to more recent explorations of artificial intelligence, algorithmic fairness, and cross-border data flows, the competition has mirrored our collective journey from awareness to advocacy, from compliance to innovation.

This volume gathers that journey. It features contributions from early voices such as Agih Sylvester Isaac and Victoria Oloni (2019); continued engagement from Asuquo Mkpoikana Joseph and Rotimi Owolabi (2020); rigorous reflections by Gabriel Temitope Omoniyi and Dorcas (Tsebee) Doowuese (2021); sustained policy analysis by Gabriel Omoniyi and Mary Omobolanle (2022); timely insights from Imoter Kelvin Kpengwa and Obiorah Victor Chibuzor (2023); and the 2024 works of Olufolajimi Otitoola and Ikenna Mba. The continuum culminates in the 2025 winning essays by Abdulganiy Olayinka Abdulganiy and Mujeebat Moyosore Idris, which probe the tensions between memory, erasure, and youth privacy in the age of artificial intelligence.

Together, these essays do more than just document ideas, they chart a story of intellectual succession: mentors guiding new voices, problems revisited as technology matures, and a community learning to transform legal principles into tools for protection, inclusion, and innovation. As Lawyard marks its tenth anniversary, we find it fitting to revisit these essays — not only as academic contributions but also as milestones in a growing national consciousness about privacy, innovation, and human dignity.

EDITOR'S NOTE

To every writer, mentor, reviewer, and reader who has sustained this tradition, we extend our deepest gratitude. May these pages inspire new generations to pursue justice and accountability, and to ensure that as technology advances, it remains firmly anchored in the service of humanity.

With gratitude and resolve,
GBOLAHAN BADMUS
Editor, Lawyard Special Privacy Edition (2025)

DANIEL ÌBÍKÚNLÉ
Co-Editor

THE INVISIBLE AUDIENCE: CAN ONLINE PLATFORMS SAFEGUARD YOUTH PRIVACY.



BY MUJEEBAT MOYOSORE IDRIS

THE INVISIBLE AUDIENCE: CAN ONLINE PLATFORMS SAFEGUARD YOUTH PRIVACY

BY
MUJEEBAT MOYOSORE IDRIS

INTRODUCTION

I remember the first time I created a social media account. I was probably too young, but all my friends were doing it. It felt like a private club, a digital treehouse where I could hang out with my friends, share silly jokes, and post photos. What I didn't realise back then was that our treehouse had no walls, and we were performing on a stage with an invisible audience of unimaginable size. This is the reality for most young people in Nigeria today. We grow up online, sharing fragments of our lives without a full understanding of who might be watching, collecting, and using our digital footprints. This essay is my exploration of a question that affects me and my entire generation: **Can online platforms actually safeguard our privacy?**

To break this down, I need to define the two key ideas in the topic. First, the **'Invisible Audience'**. This term describes the unknown and often unknowable group of people, organisations, and automated systems that can see, collect, and process the personal information a user shares online.[1] It's not just your friends; it's data brokers, advertisers, potential employers, artificial intelligence algorithms, and even malicious actors like hackers or bullies. You cannot see them, but they can see you.

Second, **'youth privacy'**. This isn't just about keeping secrets. In a legal and digital sense, youth privacy refers to the right of a minor, a person under the age of 18, to have control over how their personal data is collected, used, and shared online. [2] It's a special category of privacy because young people are considered more vulnerable. Our brains are still developing, making us more impulsive and less able to understand the long-term consequences of sharing personal information. [3] A silly photo shared at 14 could resurface and cause embarrassment when we're 25 and applying for a job.

So, when we ask, **"Can online platforms safeguard youth privacy?",** we are asking if companies like Meta (Facebook, Instagram), TikTok, Google, and Snapchat have the ability, and more importantly the willingness, to protect the personal information of their young users in Nigeria from this invisible audience. This essay will argue that the architecture of the digital economy, built upon data surveillance and engagement-at-all-costs, creates a fundamental and structural conflict of interest that renders online platforms inherently poor guardians of youth privacy. While the regulatory framework provided by the Nigeria Data Protection Act (NDPA) 2023 represents a necessary and positive intervention, its ultimate effectiveness is hamstrung by its principle-based nature which lacks specific design mandates, the nascent capacity of its enforcement institution, the intractable problem of age verification, and the opaque nature of algorithmic amplification, leaving young Nigerians exposed to an invisible audience they cannot see or control.

1. The Business of Being Watched: The Structural Conflict

To understand why platforms fail at privacy, we first have to understand how they make money. I've always known that these apps are free to use, but I never really stopped to think about the real cost. The famous saying is, **"If you are not paying for the product, you are the product."** This is the core of the problem.

Most major social media platforms rely on advertising revenue. [4] Advertisers pay platforms to show their ads to very specific groups of people. For example, a company selling new data plans from MTN or sneakers from a local brand like GTB Fashion Week wants to target Nigerian users aged 13-18 who are interested in Afrobeats and football. For the platform to do this, it needs to know a huge amount about its users. It needs to collect our data: our age, our location, what we like, what we watch, how long we watch it, who our friends are, and what we talk about.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

This data collection creates the invisible audience. My personal information isn't just stored in a vault; it is used to build a detailed profile of me. This profile is then sold to the highest bidder, not as "Mujeebat's profile," but as part of a larger group of "females, 16-18, in Abeokuta, interested in fashion."

This process is often invisible to us. We might give an app permission to access our contacts and location once, and then forget about it, but the app continues to collect that data in the background. [5]

From my perspective, this means the platform's main goal is to keep me engaged and scrolling for as long as possible so it can collect more data and show me more ads. Features like infinite scroll, autoplay videos, and personalised notifications are designed for this purpose. Safeguarding my privacy would often mean collecting less data about me, which would make their advertising less effective and less profitable. This is a fundamental, structural conflict of interest. It's like asking a pure water factory to help people diet and their success depends on the opposite.

2. The Legal Shield: A Critical Look at the Nigeria Data Protection Act (NDPA) 2023

Recognising that companies often won't act responsibly on their own, the Nigerian government has created a law to force them to protect users, especially children. The most important one is the Nigeria Data Protection Act (NDPA) 2023.[6]

The NDPA is a comprehensive piece of privacy law that affects everyone in Nigeria. It has special protections for children. It states that the processing of a child's personal data shall be done in the child's best interest. [7] Crucially, it sets the age at which a child can legally consent to data processing by themselves at 18, though it allows for a lower age to be prescribed by regulation, which has not yet happened. [8] This is a stricter standard than in many other countries. When I sign up for a new app, if I say I'm under 18, the platform is supposed to get consent from my parent or guardian.

The NDPA establishes the Nigeria Data Protection Commission (NDPC) as the regulator. The Act is based on core principles like lawfulness, fairness, and data minimisation, which mean platforms can only collect the data they absolutely need.

However, a critical analysis reveals this framework, while groundbreaking, has significant limitations. Unlike the UK's Age Appropriate Design Code which provides 15 specific design standards, the NDPA remains largely principles-based. [9] It lacks granular, mandatory rules on issues like privacy-by-default settings or the prohibition of harmful nudge techniques, leaving room for platforms to comply in name but not in spirit.

Furthermore, its effectiveness is hamstrung by the challenge of reactive enforcement. The NDPC is a new institution that must build its technical and legal capacity from the ground up to face the well-resourced tech giants it regulates. [10] This task is monumental in a country with Nigeria's vast population and limited regulatory infrastructure. Jurisdictional enforcement against foreign-based companies remains a classic hurdle in internet governance. While fines for non-compliance are potentially significant, they must be effectively imposed to act as a true deterrent. Without proactive, independent audits and swifter penalties for non-compliance, the NDPA's powerful principles risk being dormant on paper for many young Nigerians.

3. The Unresolved Legal Challenges: Age Verification and Algorithms.

Even with this new law, the invisible audience remains a constant threat because of two unresolved legal and technical challenges.

The Age Verification Paradox: The biggest weakness is age verification. The law says a platform must treat me as a child if I am under 18 and get parental consent. But how does the platform know my real age? Almost everyone I know in Nigeria who signed up for social media under the age of 18 simply lied about their birthday.

[5] *TechHive Blog, 'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

[6] *Nigeria Data Protection Act, 2023.*

[7] *Ibid s 31(1)(a)*

[8] *Ibid s 31 (2)*

[9] *Information Commissioner's Office (UK), 'Age Appropriate Design: A code of practice for online services' (2021) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ accessed 31 August, 2025.*

[10] *BusinessDay, 'Challenges and opportunities for the Nigeria Data Protection Commission' (22 July 2023) https://businessday.ng/technology/article/challenges-and-opportunities-for-the-nigeria-data-protection-commission/ accessed 31 August 2025.*

The platform asks, “When were you born?” and there is no check. You just type in a fake year. Instantly, you are now an “adult” in the system, and all the protective walls disappear. This is the critical loophole that renders many protections useless. Any proposed solution, like mandatory National Identification Number (NIN) verification, creates its own massive privacy risks by centralising highly sensitive data, a concern already debated in the context of SIM linkage in Nigeria. [11] This paradox is perhaps the single greatest legal and technical hurdle in safeguarding youth privacy online in Nigeria.

The Algorithmic Black Box: When I think of the invisible audience, I used to think only of people. But my research has shown me that the most pervasive audience is not human at all; it is the algorithmic systems that govern what I see online. This creates a major legal challenge: the "black box" problem.

Every time I open Youtube or Instagram, an algorithm is watching me. It notes what I pause on, what I like, what I share, and how long I watch a video. It uses this data to decide what to show me next. Its goal is to keep me on the app. This process is completely hidden from me. I don’t know why I am being shown a particular video or ad.

These algorithms can push users towards harmful content. If a young person feeling sad watches a few videos about depression, the algorithm might see this as a sign of engagement and start recommending more extreme content. While there is no direct Nigerian equivalent to the UK's Online Safety Act yet, the NDPC has a mandate to ensure data processing is not harmful. The potential for harm is clear and particularly acute in Nigeria's diverse society. Imagine a Nigerian teenager constantly being fed algorithmically recommended content that promotes cyberbullying, ethnic hatred, or dangerous challenges. This highlights a key legal frontier for the NDPC: how can a new regulator ever truly audit an algorithm that the platform itself claims is a proprietary trade secret? The opacity of these systems makes enforcing the "best interest of the child" principle incredibly difficult.

4. The Platform’s Defence and Its Rebuttal.

A robust defence from the platforms might argue that this critique is unfair. They would contend that they provide valuable free services to Nigeria's large and growing youth population, fostering digital inclusion and economic activity in a region where affordability is key. They would argue that overly stringent regulations could stifle innovation, limit access to information, and ultimately disadvantage the very users they are meant to protect. They would further point to their global community guidelines and terms of service as evidence of their commitment to safety.

While these points have economic merit, they ultimately fail under legal and ethical scrutiny. The argument of "innovation stifling" is often used to avoid necessary regulation. The provision of free services cannot be a licence to exploit the data and compromise the well-being of Nigerian youth. Global policies are often not tailored to specific local risks faced by Nigerian youth, such as ethnic tensions. Parental controls place an unreasonable burden on parents, many of whom are less digitally literate than their children. Most crucially, these defences ignore the core premise: that the platform’s fundamental design should not necessitate such external defences. The duty of care, as enshrined in the NDPA, must lie primarily with the service provider, not the child user or their parents. It is the architect's job to build a safe building, not the resident's to avoid collapsing floors. Economic benefits must not come at the cost of fundamental rights.

5. Towards a Robust Legal Solution in Nigeria.

Therefore, I believe that while platforms can be pushed to build higher fences, they cannot be relied upon to be the sole guardians of our privacy. True safety will come from a combination of robust and enforced regulation, a fundamental shift in platform design away from surveillance-based models, and, most importantly, a generation of young Nigerians who are educated, critical, and empowered to navigate the digital world with their eyes open to who might be watching.

[11] *Premium Times, ‘NIN-SIM Linkage: Addressing the privacy concerns’ (10 April 2022) https://www.premiumtimesng.com/opinion/443654-nin-sim-linkage-addressing-the-privacy-concerns.html accessed 31 August 2025.*

We need to move beyond the current framework to more powerful legal solutions:

- **Proactive and Strategic Enforcement by the NDPC:** Beyond capacity building, the NDPC should prioritise its initial enforcement actions on clear, winnable cases against platforms that have no meaningful age verification whatsoever, creating strong precedent and demonstrating resolve. It should also develop specific, sectoral guidelines that move beyond principles to provide actionable design rules for platforms operating in Nigeria.

- **Innovative Public-Private Partnerships:** The Commission could collaborate with Nigerian civil society organisations (CSOs) with a proven track record in digital rights, like Paradigm Initiative. These CSOs can act as force multipliers, assisting with consumer education, reporting violations, and even undertaking strategic litigation to test the boundaries of the new law.

- **Integrating Digital Literacy into National Curriculum**: Digital literacy, understanding the invisible audience, should not be a standalone subject but be woven into the fabric of existing curricula like Civic Education and Computer Studies. This would ensure a generation of Nigerians are taught from a young age to think critically about their digital lives.

- **Exploring a Stricter Liability Regime:** The government should consider exploring a strict liability standard for harms to children that are amplified by a platform's algorithmic systems, making it easier to hold them legally and financially accountable within Nigerian courts.

Conclusion.

The invisible audience is a real and persistent feature of online life for young people in Nigeria. Online platforms, driven by a need to profit from our attention and data, are structurally ill-equipped to safeguard youth privacy due to a fundamental conflict of interest.

The Nigeria Data Protection Act 2023 is a vital and welcome first step. It provides the legal framework to force platforms to make changes that can make the online world safer for my generation. However, this measure is not enough. Its principle-based approach lacks the teeth of specific design rules, and weak age verification creates a giant loophole. The unchecked, opaque power of algorithms means the most dangerous part of the invisible audience is still watching and influencing.

The potential for real-world harm is significant and particularly acute in the Nigerian context. The law has taken a vital first step but must now be activated through vigorous, strategic enforcement and complementary measures like education. The invisible audience will always exist, but through the robust and imaginative implementation of the NDPA, it does not have to be a hostile one for the Nigerian youth.

THE INVISIBLE AUDIENCE: CAN ONLINE PLATFORMS SAFEGUARD YOUTH PRIVACY

BY
PATRICK CHRISTABEL CHIAMAKA

The internet usually referred to as a "network of networks" provides an avenue for people to share information and communicate from all over the world. It is the digital playground where today's youth spend most of their time; every click, like, and scroll is quietly recorded, traded, and stored in databases they will never see. To them, the internet is a place of connection and self-expression; to the invisible audience lurking behind the screens, it is a goldmine of unfiltered, intimate data. The "invisible audience" describes a psychological state where individuals believe they are being watched by countless unseen observers; this was a concept from David Elkind's theory of 'Adolescent Egocentrism'. While originally tied to adolescent development, in today's digital age it also reflects the very real surveillance young people face from advertisers, data brokers, and algorithms.

In 2020, Irish regulators fined TikTok, a social media platform, €345 million for violating children's privacy. The Data Protection Commission (DPC) found that TikTok had not been transparent enough with children about its privacy settings, and raised questions about how their data was processed. The investigation found that accounts for users aged 13–17 were public by default, exposing their content to anyone, this was a direct breach of General Data Protection Regulation's "privacy by design" principles. This case is not an isolated incident, it is part of a global pattern where major platforms prioritize growth over safeguarding young users' privacy, often making design choices that expose minors to unnecessary risks.

It is estimated that one-third of global internet users are under the age of 18. As digital technologies increasingly mediate nearly all aspects of their lives, including their education, bringing unique opportunities and serious risks. It is imperative to ensure their well-being but perhaps rushed efforts to protect youth from risks do not significantly limit their access to valuable opportunities. Rather, these efforts must both protect and empower young people while allowing them to gradually develop autonomy and resilience.

Risks for youth online include well-known concerns such as coming across age-inappropriate content, encountering predators, and being a victim of cyberbullying or cyber harassment. Other less visible risks include commercial exploitation through profiling and behavioral advertising as well as societal shifts such as surveillance normalization, as young people may become accustomed to constantly being watched and recorded.

Social media platforms present themselves as safe spaces for creativity and connection, yet behind their colourful interfaces lies an invisible audience of advertisers, data brokers, and algorithms harvesting personal information in real time. For minors, this surveillance is not merely an invasion of privacy; it is a profound and often irreversible breach of trust.

Studies show that by the age of 13, the average child has already had over 72 million data points collected about them including browsing histories, location trails, search queries, purchasing patterns, and even biometric identifiers such as facial recognition data. Unlike adults, young users often lack the cognitive maturity and legal awareness to grasp the long-term implications of leaving such a detailed digital footprint. These digital traces can follow them into adulthood, influencing future opportunities.

Over the past two decades, social media has transformed how people connect and communicate. It was defined as online platforms that allow users to share information, opinions, and interests, it has become deeply woven into daily life, especially for adolescents and young adults, it was initially embraced for fun, messaging, and learning but social media now shapes both group interactions and individual behaviour worldwide.

In the digital age, the boundary between a young person's public and private life is vanishing at alarming speed. Social media platforms encourage constant sharing of thoughts, photos, locations, and even emotions often without users realizing how much of themselves they are giving away. For youths, whose sense of identity is still developing, this loss of privacy can have lifelong consequences.

Many platforms collect vast amounts of personal data under vague consent agreements that few young users read or understand. This data can be sold, profiled, or misused, shaping everything from targeted advertising to political manipulation.

This unseen group, 'the invisible audience, makes it hard for young people to control their personal boundaries online. They may believe they are sharing with friends, but the reality is that their audience is often much larger and different than expected. In face-to-face conversations, we know exactly who we're speaking to. Online, we can't easily tell who will see our posts, when, or in what context.

Social Networking Sites (SNSs) show that many young users are unaware of these risks, a pattern known as the 'privacy paradox'. Even with more experience, and better use of privacy settings, gaps remain due to age, gender, and digital skills. Some use creative strategies like "social steganography" to hide messages, but platform design changes can undo these protections (Stutzm. Without stronger, user-friendly privacy tools and education, invisible audiences will continue to erode the safety and autonomy of the next generation.

Social media has expanded the size and unpredictability of audiences. Content can be shared instantly, saved, and rediscovered long after posting. A Facebook update might be read immediately by one person and months later by another. This makes the audience both larger and less predictable. Ordinary users now face celebrity-like exposure. A Pew Internet report found the average Facebook user had 245 friends.

Youth privacy online is safeguarded at least in theory by a mix of national laws, regional regulations, and international treaties. These frameworks recognize that children and adolescents are especially vulnerable to exploitation. The UNCRC enshrines every child's right to privacy, encompassing their communications, home life, and reputation. The European Union mandates that personal data of a child under 16 may only be lawfully processed with parental consent; member states may lower this threshold to the age of 13.

In Nigeria, an Act enacted on June 12, 2023, provides a comprehensive framework for personal data protection. It defines a "child" as anyone under the age of 18 and requires appropriate mechanisms to verify age and obtain consent, prioritizing alignment with the Child Rights Act. The Act also established the Nigeria Data Protection Commission (NDPC) to enforce compliance and oversee data processing practices.

However, enforcement is often inconsistent, and global tech companies frequently exploit legal loopholes or jurisdictional gaps. As technology evolves faster than legislation, the real challenge lies not in drafting protections but in ensuring they are implemented effectively to shield young users from the invisible audience that profits from their data.

Online platforms recognize the heightened vulnerability of minors and have introduced various tools to enhance youth privacy and digital safety. The Age appropriate design code, also known as the Children's Code, is a British internet safety and privacy code of practice created by the Information Commissioner's Office (ICO). The Children's Code is written to be consistent with GDPR and the DPA, meaning that compliance with the Code is enforceable under the latter. It applies to any internet-connected product or service that is likely to be accessed by a person under the age of 18.

Platforms should also be required to produce comprehensive and verifiable transparency reports. These reports must include clear metrics on how many underage accounts are detected and removed, what enforcement actions are taken, and how effective parental controls and restricted modes are in practice.

Finally, international cooperation is essential. Since online platforms operate across borders, harmonizing youth privacy standards through bodies like the United Nations Internet Governance Forum would prevent companies from exploiting weaker legal jurisdictions. By combining technological innovation, legislative reform, and transnational collaboration, youth privacy protections can move from being symbolic gestures to enforceable rights.

Nonetheless, the challenge of youth privacy in the age of the invisible audience lies not only in technology's ability to expand and blur audiences, but in the structural gaps of law, policy, and awareness. Social media collapses contexts and extends the reach of content far beyond the imagined audience, exposing young users to unforeseen privacy risks, from reputational harm to data exploitation. While platform measures and existing legal frameworks offer some protection, their effectiveness is limited by loopholes, inconsistent enforcement, and the sheer unpredictability of online visibility. Addressing this requires a coordinated effort: laws must evolve to account for the realities of networked communication, platforms must design with transparency and privacy-by-default, and young people must be equipped with the digital literacy to navigate audiences they cannot see.

Protecting youth privacy in this context is not optional; it is a legal and moral necessity if we are to preserve trust, safety, and dignity in the digital public sphere. Only through such a holistic approach can the promise of social media be reconciled with the rights and security of its youngest participants.

It requires online services to be designed in the "best interests" of children and their health, safety, and privacy, requiring that they be afforded with the strongest privacy settings by default, that only data strictly necessary to deliver individual service elements is collected from children unless there is justification, and that children's personal data not be disclosed to third-parties unless there is justification.

Some platforms like TikTok offer a Family Pairing feature that links parent and teen accounts, enabling parents to set screen time limits, manage direct messaging, restrict content by keywords, and tailor comment settings. These are executed via digital prompts and customizable rules. Introduced in 2020, this feature lets parents oversee screen time, manage privacy features, and restrict interactions. More recently, enhanced controls allow parents to block specific accounts and receive alerts when teens upload contents.

Also, Instagram Teen accounts (13-17 years) automatically have a protected experience, with built-in limits on who can contact them and the content they see, plus more ways to connect and explore their interests. Teen Accounts are automatically set to private, teens under 16 can only change this default setting with help from a parent or guardian and there accounts are put on silent from 10pm to 7am.

YouTube has equally built a platform called YouTube kids. YouTube Kids is an American video app and website developed by YouTube, a subsidiary of Google. The app provides a version of the service oriented solely towards children, with curated selections of content, parental control features, and filtering of videos deemed inappropriate for viewing by children under the age of 13, in accordance with the Children's Online Privacy Protection Act, which prohibits the regular YouTube app from advertising to children under the age of 13.

However, these measures face significant limitations. Fake age sign-ups remain widespread, as children can easily bypass verification systems by entering a false birthdate. Terms of Service often contain loopholes, using vague language that allows continued data collection even when restrictions are in place. Furthermore, transparency reports from major platforms are frequently incomplete, making it difficult for regulators and the public to assess the true effectiveness of youth privacy measures. Without robust enforcement and technological improvements, these tools, while well-intentioned, cannot fully address the risks faced by minors in digital spaces.

While existing measures by online platforms demonstrate a commitment to safeguarding young users, persistent loopholes and enforcement gaps necessitate stronger interventions. A first step is the implementation of robust, verifiable age verification systems that go beyond self-reported data. Technologies such as AI-powered facial age estimation, adopted in partnership with Instagram, could be integrated across major platforms. This would make it significantly harder for minors to falsify their ages, while still protecting user anonymity through privacy-preserving verification methods.

Secondly, parental control features must evolve into collaborative safety tools rather than purely restrictive mechanisms. Current systems like TikTok's Family Pairing could be enhanced with transparent activity reports, educational prompts about online safety, and the ability for both parent and child to set mutual boundaries an approach aligned with UNICEF's advocacy for digital literacy as a shared responsibility.

Furthermore, data minimization must be legally enforceable. Existing privacy policies should be backed by statutory frameworks which impose fines for unlawful collection and use of children's data.

Nigerian lawmakers could adapt similar standards under the Nigeria Data Protection Act 2023, with specific clauses on children's online privacy.

THE INVISIBLE AUDIENCE: CAN ONLINE PLATFORMS SAFEGUARD YOUTH PRIVACY

BY
OBETA RUTH OLUCHI

1.0 INTRODUCTION

According to the United Nations International Children's Emergency Fund (UNICEF), over 71% of youths aged between 15 and 24 are online worldwide, making them the most connected group in the world. Without a doubt, the proliferation of social networks and other online platforms in today's digital age has led young people to spend significant portions of their lives online, thereby leaving digital footprints that are constantly tracked and monitored by online spectators, including the "invisible audience." This refers to people who consume their online content but cannot be seen or easily identified. While online platforms can be used to promote connectivity, education, and self-expression, they also expose youth to privacy issues. The question of interest therefore emerges: Can online platforms safeguard youth privacy? This essay examines the current legal frameworks, and evaluates case studies as well as real-life practices to determine whether online platforms can truly safeguard youth privacy in this era of digital connectivity and in the face of the invisible audience. It further recommends strategies for protecting youth privacy and well-being in today's digital age.

2.0 GENERAL OVERVIEW: UNDERSTANDING THE INVISIBLE AUDIENCE

A look into history reveals that what is known today as the invisible audience originated from the term imaginary audience, coined in the 1960s by the psychologist David Elkind. The imaginary audience describes the mindset of a teenager convinced that every action, such as sneezing in class is being observed and judged by a crowd that cannot be seen.

It is further described as "a hallmark of adolescent egocentrism, where self-obsession reigns supreme and the teenage brain blurs the line between "some are watching" and "everyone must be watching."

Fast-forward to the digital age: that once imaginary crowd has metamorphosed into the "Invisible Audience—the hazy mass of followers, lurkers, silent readers, and "should-be-watching people" who occupy the background of young people's online lives.

Unlike Elkind's imaginary audience, which existed only in the mind of the adolescent, today's invisible audience is both psychological and real. Every post, picture, or video uploaded online is potentially viewed by strangers, silent friends, data miners, advertisers, or even malicious actors; none of whom are visible to the user.

Michael S. Bernstein etal, in their article titled "Quantifying the Invisible Audience on Social Networks," observed that "Posting to a social network site is like speaking to an audience from behind a curtain. The audience remains invisible to the user: while the invitation list is known, the final attendance is not. Feedback such as comments and likes is the only glimpse that users get of their audience, and that audience varies from day to day".

For instance, anyone who has an active LinkedIn account should be familiar with the "Who Viewed Your Profile?" feature. The platform records all profile visits but only shows a partial list to free users, urging them to pay for Premium to see more details of their audience. Through this feature, users know they are being watched by an invisible audience but they cannot fully know who is watching unless they pay, and even then, only partially.

The invisible audience is no longer a figment of teenage imagination; it is a built-in feature of the digital world. Picture a young person posting a photo online, believing that it will circle only among online friends. In reality, that photo stretches far beyond, and can reach unknown individuals and corporations. The invisible audience can therefore be said to be a powerful force in shaping the behaviour, identity and online privacy of the youth.

3.0 LEGAL AND POLICY FRAMEWORKS FOR PROTECTING YOUTH PRIVACY

Privacy is a fundamental human right, and is recognized in International Law. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights provide that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

In Nigeria, Section 37 of the 1999 Constitution provides for the right to privacy. in the case of Olatokun v. Polaris Bank, the Lagos State High Court awarded damages against Polaris bank for breaching the plaintiff's privacy rights through sending unsolicited messages after he closed his account with the bank.

Additionally, the Nigeria Data Protection Act (NDPA) 2023, created the Nigeria Data Protection Commission (NDPC) and provided comprehensive provisions for privacy protections, especially for minors or underaged children. The NDPA provides strict penalties for violations and establishes mechanism for victims to lay their complaints.

Likewise, the Child Rights Act 2003, provides that "the best interests of the child" should be a primary consideration. Applied to the digital age, it can be inferred that this law makes it a duty for online platforms to come up with policies that protect young users from all forms of online exploitation including data breaches, unsolicited messages or anything that infringes on their privacy. Globally, the European Union's (EU) General Data Protection Regulation (GDPR) goes further by restricting how children's data can be processed. The regulation requires parental consent in certain cases, and imposes heavy fines for violations.

4.0 CAN ONLINE PLATFORMS SAFEGUARD YOUTH PRIVACY?: CASE STUDIES

With regards to safeguarding youth privacy, online platforms occupy a paradoxical position: on the one hand, they claim to protect youth privacy through privacy settings, parental controls, and reporting systems, on the other hand, their profit models often depend on the very practices that compromise privacy.

The tension between safeguarding youth privacy and monetizing their data lies at the core of "surveillance capitalism," a term popularized by Harvard professor Shoshana Zuboff who described it as the commodification of personal data of users by tech companies for profit making.

For instance, online platforms usually harvest youth data, including browsing histories, facial images, geolocation, and behavioural patterns to fuel targeted advertising worth billions of dollars. A 2022 report by the Human Rights Watch revealed that educational apps used during COVID-19 lockdowns secretly shared children's data to ad-technology companies.

Recently, several privacy scandals involving the misuse of youths online data have shown that young people remain vulnerable to the invisible audience. For example, in 2023, the European Union fined TikTok $370 million for mishandling children's data. Similarly, the 2018 Facebook's Cambridge Analytica scandal exposed how third-party apps harvested the data of millions, including youths, for political manipulation. Additionally, YouTube algorithms that were designed to maximize engagement of users have been accused of pushing harmful or age-inappropriate content to minors that use the application. In the same vein, Google recently settled for a fine of $30 million over allegations that YouTube illegally collected children's data without their parents' consent.

This is not just a foreign problem, it is a Nigerian reality too. In 2024, the Federal Competition and Consumer Protection Commission imposed a fine $220 million on Meta Platforms Inc. for infringing on users' data, some of the infringements include: denying Nigerians the right to control their data, transferring and sharing Nigerian user data without authorisation, discriminating against Nigerian users compared to users in other jurisdictions and abusing their dominant market position by forcing unfair privacy policies. Recently, the Nigeria Data Protection Commission also imposed a fine of $32.8 million on Meta Platforms for unauthorized processing of sensitive personal data, including those of minors.

Most disturbingly, the "invisible audience" also includes online predators. The BM Boys Sextortion Scandal demonstrated how online networks exploited TikTok and Instagram to lure teenage boys into sharing intimate content, later used to blackmail them, leading to several suicide cases amongst teenage boys. This case shows that the invisible audience is not limited to advertisers and lurkers but can include criminal predators hidden behind online anonymous accounts.

At this juncture, it is clear that the challenge is not whether online platforms can safeguard youth privacy since their technology and privacy settings already allows it. The true question is whether governments, regulators, and individual users of these online platforms have the will to demand it. Until that happens, the invisible audience will remain a constant threat, profiting from the very youths that online platforms claim to protect.

5.0 CHALLENGES AND BARRIERS IN PROTECTING YOUTH PRIVACY

The challenges militating against the protection of youth privacy in this age of the invisible audience include:

5.1 Low Digital Literacy and Awareness

A major challenge to protecting youth privacy in the digital age is the low level of awareness among youths regarding their digital rights.

Many young people are active users of online platforms, but only a handful of youths understand how their data is collected, processed, and monetized. As a result, they often give consent without reading terms of service, share sensitive information without thinking twice, and they usually fall prey to phishing attacks or scams.

5.2 Cross-Border Jurisdiction Issues

In developing countries like Nigeria, most online platforms that are popular among youths are owned by foreign corporations. These companies often operate outside the shores of Nigeria, thus making the enforcement of national privacy laws against such companies difficult.

While the Nigerian Data Protection Act (NDPA) of 2023 attempts to address this by regulating companies and platforms that are in charge of processing Nigerian citizens' data, the practical enforcement of the Act against multinational tech giants and online platforms remains a difficult task because of issues associated with cross-border jurisdiction.

5.3 Gaps in Youth or Child-Specific Protections

Although the Child Rights Act of 2003 provides a general framework for the protection of minors, it has not been fully domesticated across all Nigerian states. Also, its application to online spaces is limited, thereby leaving children and teenagers exposed to infringement of their online data, and issues such as online grooming, and exploitation.

6.0 RECOMMENDATIONS AND CONCLUSION

The promise of the digital age is that it connects, empowers, and informs. Yet for youths all over the world, the same platforms that enable self expression and connectivity also expose them to an invisible audience of advertisers, corporations, predators, and even government organizations; people who are constantly watching, tracking, and in some cases exploiting their data and online activities.

This paradox cannot be ignored as a society that fails to protect the online safety of its young people is a society that compromises its own future.

Several countries like Nigeria have taken commendable steps by enacting laws and policies for regulating online privacy but laws on paper cannot, by themselves, shield a teenager who unknowingly clicks "I agree" on a privacy policy, or a child coerced into sextortion. Therefore, protecting youth privacy in this age of the invisible audience requires a multi-stakeholder approach that goes beyond self-regulation.

To this end, it is recommended that Governments should strengthen data protection laws and enforce compliance with multinational corporations. In Nigeria, the Nigeria Data Protection Commission (NDPC) should be properly funded and empowered to monitor and sanction data and privacy violations, including those by online platforms operating in the country. International cooperation and collaboration with data protection authorities, is also necessary to address cross-border enforcement challenges.

In the same vein, schools, parents, and Non-governmental Organizations (NGOs) should integrate digital literacy into their curricula. Digital literacy must become as essential in schools as Mathematics and English. There should also be widespread awareness campaigns targeted at ensuring that young people understand the risks of oversharing their information online and the realities of the invisible audience.
Again, online platforms themselves should also increase transparency and accountability by publishing clear reports on how youth data is collected, used, and shared. They should also simplify privacy controls to make them accessible to young users.

In conclusion, if the invisible audience continues unchecked, today's youth may grow up not as digital natives, but as digital captives. Safeguarding youth privacy is therefore not optional; it is the price of protecting our future and it calls for collective efforts.

THE ERASURE PROBLEM: RECONCILING THE RIGHT TO BE FORGOTTEN WITH THE IMMUTABILITY OF AI MODEL TRAINING DATA

BY

ABDULGANIY OLAYINKA ABDULGANIY

INTRODUCTION

The twin principles of the Right to Erasure (RtE) and the Right to be Forgotten (RtBF) have become defining features of modern data protection law, advancing human dignity and informational autonomy in a digital ecosystem where memory is effectively permanent. While distinct, the two are closely connected: RtE is the codified, procedural right to request deletion of personal data, whereas RtBF represents the broader jurisprudential idea that individuals should not be perpetually defined by outdated or irrelevant information. However, the emergence of artificial intelligence, particularly large-scale machine learning models trained on heterogeneous datasets, raises profound questions about the feasibility of enforcing these rights, given the structural resistance of such technologies to erasure. This essay contends that while the RtBF must remain robust, its application must be recalibrated to reflect the technical realities of AI, through proportionate, context-sensitive policy solutions.

LEGAL FRAMEWORK: THE RIGHT TO ERASURE

The juridical ancestry of the RtBF can be traced to the continental European tradition of "droit à l'oubli" (right to oblivion), which historically allowed rehabilitated offenders to move beyond their past transgressions without perpetual public scrutiny. In the digital age, however, the permanence and searchability of online information have given this principle renewed urgency, as individuals increasingly find that outdated or prejudicial data can indefinitely shape their reputations and opportunities. Early legislative recognition of erasure emerged in the Data Protection Directive 95/46/EC, which provided for the rectification or removal of incomplete, inaccurate, or unlawfully processed data.

However, the jurisprudential lineage of the RtBF is most aptly traced to the Court of Justice of the European Union's (CJEU) landmark decision in Google Spain v. González (Google Spain Case).

In Google Spain, the CJEU confronted a request by Mario Costeja González to delist links from Google search results pointing to a decades-old newspaper notice about his past social security debts. The CJEU held that search engines, by collecting, indexing, and making available personal data, engage in "processing" and act as "data controllers," even where the information is lawfully published by third parties. This expansive interpretation reframed search engines as powerful intermediaries whose structuring of information can profoundly affect privacy. Crucially, the Court found that even accurate and lawfully disseminated information may, over time, become "inadequate, irrelevant, or excessive." In such cases, the individual's rights under Articles 7 and 8 of the EU Charter override both the economic interests of the search engine and the public's right of access, save where compelling public interest justifies continued accessibility (for example, when the data subject is a public figure). This reasoning established that de-listing obligations are independent of the continued lawful publication of content at source, thereby reframing privacy as the right to prevent information from remaining ubiquitously accessible via search engines.

Piggybacking on the doctrinal momentum of Google Spain, the European legislature codified the Right to Erasure in Article 17 of the General Data Protection Regulation (GDPR), which became directly applicable across the Union in May 2018. Article 17(1) entitles data subjects to obtain erasure "without undue delay" where one of six grounds applies: the data is no longer necessary for its original purpose; consent has been withdrawn; a successful objection under Article 21 has been lodged; the processing is unlawful; erasure is required to comply with legal obligations; or the data was collected from a child.

Article 17(2) introduces the so-called "cascade" obligation, requiring controllers who have made data public to take reasonable steps to inform other controllers of the erasure request, subject to feasibility and proportionality. At the same time, Article 17(3) tempers the right by carving out exceptions for freedom of expression, legal compliance, public health, archiving, research, and legal claims, ensuring the right does not operate as an unchecked tool of censorship. In this way, the GDPR codification reflects both the expansive vision of Google Spain and the necessity of balance with competing fundamental rights under the EU Charter.

Despite its normative ambition, the RtBF has attracted sustained criticism. Commentators argue that the Court's open-textured criteria "inadequate, irrelevant, or excessive" are conceptually vague, producing inconsistent outcomes across Member States and forcing search engines to act as de facto arbiters of privacy versus public interest. Scholars such as Allegri describe the right as "contourless and indeterminate," while others warn that delegating balancing exercises to private intermediaries risks privatising censorship, undermining democratic accountability, and incentivising over-compliance. Critics like Katsirea and De Baets caution that the right may suppress uncomfortable truths, enable reputational whitewashing, and foster an Orwellian "memory hole." Practical limitations also persist: delisting is territorially confined to the EU, meanwhile, data often re-emerges on non-EU domains or caches, and immutable technologies such as blockchain and AI models render true deletion elusive.

Post-GDPR case-law also reveals both convergence and divergence in national courts' balancing methodologies. Courts in France and the Netherlands have emphasised a nuanced, case-by-case balancing, while the UK High Court in NT1 & NT2 v Google LLC granted erasure in one case but refused it in another, illustrating that outcomes turn heavily on factual context and the perceived legitimacy of continued public interest. The CJEU itself, in Google v CNIL, resisted extending the RtBF globally, holding that delisting obligations apply only within the EU.

This decision reflects an awareness of both comity concerns in international law and the practical impossibility of imposing a universal erasure mandate in a borderless digital environment.

A persistent tension also exists between the jurisprudence of the CJEU and the European Court of Human Rights (ECHR). The CJEU has often prioritised data protection and privacy, whereas the ECHR has leaned toward freedom of expression and access to information. In M.L. and W.W. v Germany, the ECHR refused to require anonymisation of convicted murderers' names in online archives, ruling that the public's right to information outweighed privacy claims. Conversely, the Italian Court of Cassation has held that anonymisation may prevail in purely historiographical contexts unless renewed public interest arises or the individual remains a public figure. These divergent approaches reveal the underlying fragility of the RtBF: while intended as a shield for dignity, its scope is inherently context-bound and vulnerable to manipulation.

RtBF Beyond Europe

Although most fully developed under the GDPR, the RtE now spans jurisdictions, each tailoring it to local legal and cultural contexts. In California, the CCPA/CPRA grants consumers deletion rights and obliges businesses to cascade requests to service providers, reflecting an explicitly consumer-centric orientation. Brazil's Lei Geral de Proteção de Dados (LGPD) hews closely to the European model, allowing deletion where processing is unlawful or consent withdrawn, subject to narrowly drawn exceptions for compliance and regulatory necessity. South Korea's PIPA takes a more muscular approach, mandating demonstrable, irreversible destruction absent a lawful retention ground.

South Africa's POPIA, by contrast, adopts broader triggers — data that is inaccurate, irrelevant, excessive, or unlawfully obtained, while preserving exceptions for compliance and public interest.

Nigeria's trajectory reflects both convergence with and divergence from these models. Having pioneered data protection in West Africa through the NDPR 2019, it has now consolidated its framework in the Nigeria Data Protection Act 2023 (NDPA). Section 34(1)(d) expressly establishes a right to erasure where data are obsolete, incomplete, or no longer necessary, alongside grounds familiar from Article 17 GDPR such as unlawful processing, withdrawal of consent, and legal obligations. The Act's exceptions similarly echo the European framework, encompassing freedom of expression, research, archiving, and legal claims. Enforcement is entrusted to the Nigeria Data Protection Commission (NDPC), which is empowered to issue compliance orders and sanctions.

Similarly, a cascade obligation, modelled on GDPR Article 17(2), requires controllers who have shared data to take "reasonable" steps to notify third parties of erasure requests. Yet, the Act gives little guidance on what counts as reasonable technological effort in a distributed, cloud-based environment. Despite its alignment with global best practice, the Nigerian framework suffers from unresolved ambiguities. The Act does not define what constitutes "deletion," leaving open whether logical deletion, encryption, or irreversible anonymisation will satisfy statutory requirements.

Codes of practice envisaged under section 64 potentially the vehicle for clarifying such issues remain in draft, depriving controllers of much-needed guidance on secure destruction or on emerging challenges such as model editing and machine unlearning in AI contexts. More fundamentally, infrastructural deficits weaken enforcement: smaller controllers often lack audit trails or version-control systems capable of demonstrating erasure across multiple platforms and cloud regions.

Across these jurisdictions, three common denominators emerge. First, the right is never absolute: every statute embeds substantive or public-interest exceptions, including freedom of expression, legal obligations, research, or journalistic privilege. Second, erasure must be demonstrable and technically effective; mere deactivation or suppression is insufficient, as controllers must show that data is either irreversibly destroyed or rendered incapable of re-identification. Third, most regimes impose a cascade obligation, requiring controllers to extend erasure requests downstream to processors or service providers, thereby ensuring compliance throughout the supply chain. Together, these elements reflect a nascent global convergence on the normative core of data erasure, even as differences of scope, enforcement, and emphasis persist across jurisdictions.

the Immutability of AI Model Training Data & The Erasure Problem

The rapid proliferation of large-scale AI models trained on vast, heterogeneous datasets presents the most intractable challenge to enforcing the RtBF and RtE. Unlike conventional databases, where a record can be located and deleted, machine-learning systems do not store personal data as discrete entries. The stochastic nature of model training compounds the difficulty. Random shuffling, parameter initialisation, and parallelisation mean that retraining a model rarely produces identical results. With today's massive architectures, hundreds of layers and billions of parameters tracing or reversing the influence of one data point is computationally infeasible. As Popowicz-Pazdej notes, such architectures inherently "resist the notion of forgetting." This practical impasse, commonly referred to as the erasure problem, illustrates the clash between the legal and ethical imperative to forget versus the structural realities of technologies designed to remember.

The erasure problem stems from the way models internalise and retain information. While they sometimes memorise data verbatim, making targeted interventions like blacklisting or fine-tuning possible. Yet, such instances are rare; in most cases, the imprint is diffuse, latent, and practically irretrievable. Similarly, efforts at 'machine unlearning' algorithms designed to unwind the influence of specific data points show promise but remain computationally costly, performance-degrading, and incapable of guaranteeing complete erasure. Other safeguards are partial at best: differential privacy limits memorisation at training but sacrifices accuracy and offers no retroactive remedy, while federated learning decentralises storage but reproduces the same persistence once local updates are aggregated.

Second, although "machine unlearning" has emerged as a promising frontier developing algorithms to selectively unwind the influence of particular data points—existing techniques remain computationally expensive, performance-degrading, and lack guarantees of complete erasure. Differential privacy offers another partial safeguard, limiting memorisation at the point of training by injecting statistical noise, but it reduces accuracy and cannot retroactively cleanse models already trained. Likewise, federated learning decentralises data storage, thereby enhancing sovereignty, but once local updates are aggregated into a global model, the same persistence of influence reappears.

The compliance dimension is equally fraught. Effective implementation of the RtBF presupposes robust data provenance, that is, knowing which data trained which model, and maintaining metadata trails sufficient to scope and execute erasure requests. In practice, few developers maintain such granular records, and the brute-force alternative is retraining models from scratch without the impugned data, which is prohibitively costly and operationally infeasible. The resulting trade-off is stark between the legal ideal of digital redemption and the technical and economic realities of model development.

Although the RtBF may seem practically unenforceable in the context of machine learning, this essay contends that it must be reimagined, preserving its normative promise while remaining workable within the technical realities of AI. The next section considers how such a reconciled regime might be achieved.

Practical Recommendations

Reconciling RtBF with model immutability requires law and policy that reflect technical realities while protecting privacy. Below are practical, implementable frameworks that balance enforceability with technical realism:

Mandatory Provenance and Metadata at Ingestion

Erasure begins with traceability. As a foundational safeguard, controllers should be legally required to maintain dataset registries and structured metadata at ingestion, recording attributes such as source, consent status, sensitivity classification, retention period, and any RtBF flags. Developers must, in turn, preserve a verifiable mapping between dataset versions and model iterations. With this evidentiary infrastructure mandated, it will be the linchpin that renders the RtBF even conceptually enforceable in an AI environment.

Duty to Attempt Technical Unlearning

Given the stochastic and entangled nature of model training, perfect erasure is often unattainable. However, controllers should bear a documented duty to attempt technical unlearning, guided by proportionality. At minimum, this requires: (i) a recognised unlearning attempt, (ii) verification tests evidencing reduced influence, and (iii) disclosure of results to the data subject. In high-risk contexts, successful unlearning should be a precondition for deployment or continued use. This reframes unlearning as an auditable duty of effort, rather than a guaranteed cure.

Contractual Flow-Down and Model Supply-Chain Obligations

The distributed nature of AI development spanning cloud providers, data brokers, and licensors of pre-trained models means that erasure obligations must travel with the data. Controllers should embed enforceable contractual duties across their supply chains, requiring all parties to honor deletion requests, preserve provenance metadata, provide verifiable proof of deletion or unlearning, and accept proportionate audits. Where models are licensed, terms should mandate certified unlearning or compensation for retraining costs. Regulators can promote standardization through model contractual clauses, ensuring that legal obligations are not lost in the complexity of the AI value chain.

Use of Regulatory Sandboxes and Phased Obligations

To reconcile innovation with accountability, regulators should establish sector-specific sandboxes where deletion techniques and certification protocols can be trialed under controlled conditions. For critical public-interest applications (e.g., health, safety), narrowly tailored, time-limited carve-outs may be justified, provided they are paired with enhanced safeguards and full transparency. This phased approach allows regulatory expectations to mature alongside technological feasibility, ensuring that the law remains both principled and adaptive.

Transparency Obligations: Model Cards and Provenance Logs

Finally, transparency is essential for both regulatory oversight and data subject empowerment. Controllers should adopt model cards that disclose: (a) whether personal data were used in training; (b) the proportion of such data; (c) whether differential privacy was applied; (d) whether deletion is supported; and (e) the material limits of deletion. An auditable provenance ledger should record key lifecycle events from training datasets, model versions, deletion requests, and be available to regulators upon request. These measures reduce disputes, foster trust, and enable informed choices by data subjects.

Conclusion

Reconciling the Right to Erasure with the structural immutability of AI training data admits no perfect solution, but impossibility is not an option; individual dignity demands that law and policy continue to press against the technical grain. The task is not rigid absolutism but pragmatic recalibration anchored in provenance, reinforced through contractual flow-downs, operationalised via unlearning, and rendered transparent through model cards and audit trails. Proportionate, context-sensitive obligations can preserve the normative core of the RtBF while keeping innovation viable.

THE ERASURE PROBLEM: RECONCILING THE RIGHT TO BE FORGOTTEN WITH THE IMMUTABILITY OF AI MODEL TRAINING DATA

BY
CHIJIOKE UCHEAKONAM

1.0 INTRODUCTION:

The rise of artificial intelligence (AI) has revolutionized the landscape of information processing, delivering unprecedented efficiency, predictive power and even scalability. Yet, this transformation exposes a deep fault line between legal rights and technical realities – most notably the tension between the "right to be forgotten" (RTBF) and the immutability of AI training data. While the RTBF grants individuals the power to demand deletion of personal data, machine learning models embed such training data into weight distributions and parameter spaces, rendering erasure neither straightforward nor possible without retraining the entire system.

This erasure problem is far from theoretical. It raises existential questions about the enforceability of human rights in an era where AI models embed human traces within their very architecture. The implications extend well beyond academic debate. It strikes at the core of biomedical research repositories, facial recognition databases and large language models (LLMs) – all of which demonstrate how data, once learned, resists deletion. How, then, can the law expect erasure where technology renders 'forgetting' nearly impossible? This essay examines the basis of the RTBF, explores the nature of its incompatibility with AI, and assesses potential mechanisms for reconciliation.

2.0 THE LEGAL FOUNDATION OF THE 'RIGHT TO BE FORGOTTEN'

The RTBF as formally codified in Article 17 of the GDPR, is traceable by its roots in the jurisprudence of the Court of Justice of the European Union (CJEU).

Its doctrinal foundation lies in the case of Google Spain SL, Google Inc v. AEPD, Mario Costeja González where the Court held that individuals may compel search engines to delete links to information that are irrelevant or outdated, even where such information was lawfully published. The underlying rationale for this is highly philosophical.

It hinges on the theory that in a digital society where information persists infinitely, individuals must have the capacity to protect their reputation, curate their identities and move beyond past mistakes. Without such rights in place, the internet risks stripping individuals of autonomy over their own narrative and subsuming them to the permanence of digital memory.

Nonetheless, the RTBF has been a subject of controversy since its inception. Critics argue that it undermines freedom of expression, conflicts with the public's right to know and imposes heavy burden on platforms that act as intermediary of information. Yet, despite these concerns, the RTBF has entrenched itself in European privacy law as a central safeguard of international self-determination. This reflects the distinctive nature of European jurisprudence which emphasizes dignity and reputation as opposed to American traditions which prioritize free speech. Importantly, the practical operations of the RTBF have been most viable in the context of search engines, where delisting internet links severs the connection between a name and information without erasing the underlying data. However, this model of functionality is far less tractable and difficult when applied in the context of AI model learning. To truly understand this difficulty, it is necessary to consider how AI models are trained.

3.0 THE PERSISTENCE OF DATA IN AI MODEL LEARNING

Unlike traditional databases, machine learning does not preserve data points as discrete or retrievable records. Rather, training involves adjusting millions or billions of parameters to capture statistical relationships within data.

Once training is finalized, the model retains only diffused mathematical representations embedded across weight distributions. For instance, LLMs may rephrase or reproduce stylistics patterns of scraped internet text without ever 'storing' those texts in identifiable form. Similarly, a facial recognition system does not retain photographs; it encodes them as high-dimensional vectors capable of reconstructing features even after the source images have been deleted.

The implications for the RTBF are profound. Deleting an individual's data from storage does not excise its imprint from the trained model. Empirical studies have demonstrated that LLMs and generative AI systems can, under certain circumstances, regenerate training materials verbatim including names, phone numbers, or entire paragraphs from documents. Such gaps reveal the illusion of deletion, showing that even when an underlying record has been removed, its statistical shadow continues to persist.

The result is a structural asymmetry. The law assumes erasure to be technically feasible, whereas AI systems are built around permanence. This tension crystallizes the 'erasure problem' where individuals may be denied the full extent of their legal rights, not because of unwillingness, but because of structural challenges in how AI functions. For subjects, this undermines the enforceability of the RTBF and corrodes public trust in digital technology. For companies, it generates legal uncertainty, exposing them to potential liability despite good-faith efforts to comply with the RTBF. At its core, this conflict is not merely technical but normative, raising questions about whether established human rights framework – most prominently Article 8 of the European Convention on Human Rights – can adapt to emerging technologies.

4.0 WHY THE RIGHT TO BE FORGOTTEN AND AI COLLIDE: STRUCTURAL AND LEGAL TENSIONS

The RTBF is not an absolute right. Data subjects are required to ground their requests within the conditions set out in Article 17(1) of the GDPR, and even when such conditions are satisfied, the GDPR recognises certain countervailing interests that may override erasure.

In this sense, it may be argued that the GDPR itself provides the basis for much of the existing friction.

4.1 Legal Interpretation of Erasure

The GDPR grants data subjects the right to request the erasure of personal data under Article 17. However, the legal meaning of "erasure" remains conceptually imprecise and technologically underdetermined. Erasure is not defined as a stand-alone act, but as a form of processing. While the GDPR identifies substantive grounds that may trigger the right to erasure, it fails to becomes acute when applied to AI models, where erasure may be interpreted as requiring not only the deletion of raw input data but also the neutralization of its residual influence on trained model parameters.

Moreso, Article 12(3) of the GDPR states that request for data deletion must be carried out "without undue delay". This introduces a procedural dimension. It also mandates that data controllers take reasonable steps to inform other controllers who are processing the same data of such requests, thereby creating a relational obligation outside the scope of internal erasure. On the one hand, these requirements are particularly burdensome for AI systems, given the opacity of model behavior and the technical difficulty of determining whether a specific data point continues to exert residual influence after training. On the other, the practical application of the RTBF under Article 17 introduces not only legal uncertainties, but some significant practical and financial burdens for developers as well, making it difficult for data controllers to comprehensively oblige with the provisions of Article 12(3). One possible solution is full model retraining, in which the personal data is removed, and the model erased. But this is both costly and often impractical, especially for large-scale AI systems built on vast amounts of data.

4.2 Personal Data covered by the GDPR

The threshold question for determining the applicability of the GDPR to AI systems is whether the data at issue qualifies as personal data within the definition of the GDPR.

Article 4(1) of the GDPR adopts a deliberately expansive meaning, encompassing "any information relating to an identified or identifiable natural person (data subject)." This definition does not confine itself to direct identifiers such as names or national identification numbers; it extends to any form of data which, when combined with other reasonably accessible information, may enable re-identification.

The European Data Protection Board, on its part, emphasizes that identifiability must be assessed in light of "all the means reasonably likely to be used" by any actor, not merely the data controller. The CJEU has repeatedly endorsed this rational approach. In Peter Nowak v. Data Protection Commissioner, the Court ruled that exam answers and examiner comments constituted personal data because they reflected the knowledge, reasoning, and achievements of an identifiable individual.

More recently, in *Gesamverband Autoteile-Handel v. Scania,* a vehicle identification number was recognized as personal data, not intrinsically, but because it could be combined with other datasets to trace an individual. These interpretations, when transposed into the AI domain, make it increasingly difficult to enforce the RTBF.

Empirical research demonstrates that trained AI models are not immune to re-identification risks. Following the CJEU's reasoning in *Nowak*, *Gesamverband* and subsequent cases, the decisive factor is not the formal structure of the data, but the reasonable likelihood of re-identification given current and foreseeable technological means. Applied rigorously, this functional approach compels the conclusion that trained AI models, at least in some configurations, do fall within the scope of the GDPR. This brings them into direct tension with Article 17's right to erasure, since deletion of raw training data does not eliminate the residual personal imprint embedded in the model parameters.

4.3 Technical Architecture of AI Models

The technical nature of many AI models poses significant barriers to fulfilling the obligation of compliance. In machine learning systems, large datasets are incorporated during the training stage, and the data is then split into multiple datapoints.

These are then weighted and incorporated into parameter adjustments through iterative updates and spread across interconnected parameters. Due to this, performing technical removal or "forgetting" of a subject's personal data becomes far more complicated than merely deleting a file. This issue stems from the fact that AI models embed data across diverse parameters, making ad hoc erasure technically demanding. This is reinforced by the fact that data remnants may still influence a model's parameters, even after the original dataset has been purged.

5.0 Reconciling the Right to be Forgotten and the Immutability of AI

The structural impasse between RTBF and AI raises a normative dilemma: if conventional deletion is technically infeasible, should the law not require innovation-driven solution? When erasure mechanisms prove to be insufficient in addressing the persistence of personal data within AI systems, then more advanced technical strategies become necessary. A prominent recommendation is Machine Unlearning.

This refers to the design of algorithms which are capable of selectively neutralizing or erasing the impact of data points on an already trained model. Unlike full model retraining, which requires erasing the model entirely and starting the training process afresh, machine unlearning would help to surgically excise the contribution of relevant data, thereby significantly decreasing the computational and financial burden of complying with Article 17 of the GDPR.

One peculiar paradigm to this system is the SISA (Sharded, Isolated, Sliced and Aggregated). The SISA method of machine unlearning operationalizes erasure requests by splitting datasets into smaller shards, training separate models on each shard and combining their various outputs. In practice, this design would allow the removal and retraining of only those shards which contain the contested personal data, rather than retraining the entire model.

From a normative standpoint, machine unlearning aligns with Article 5(2) of the GDPR, insofar as it enhances transparency of compliance measures and traceability of data use. Moreover, in alignment with the EU AI Act 2024, AI developers are required to maintain detailed documentation of training data which would enable better tracking of personal data and more targeted removal where feasible.

Another proposal is the adoption of differential privacy as a mechanism for reconciliation. This technique introduces calibrated 'noise' into the training process of a machine learning model with the objective of obscuring the influence of any single data subject on the final parameters. This will ensure that the inclusion or exclusion of a particular data of an individual cannot be reliably inferred from the model's output. In practice, this can be achieved by fine-tuning the level of 'noise' injected at different stages of AI model training. Thus, by constraining the extent of individual records in parameter updates, differential privacy can help to mitigate the residual imprint of personal data within trained models and decrease the probability of re-identification risks.

Thus, with proper calibration, AI models can reach a level of controlled trade-off between privacy preservation and model utility. This will ensure that external observers are unable to determine, with statistical confidence, whether a person's data was present in an AI training set.

Moreover, differential privacy aligns with the safeguards under the GDPR. It resonates with the principle of data protection by design and is by default enshrined in Article 25 of the GDPR. In this sense, adopting differential privacy can serve as demonstratable evidence of good-faith efforts towards compliance.

Globally, different jurisdictions approach the erasure problem divergently. In the US, the First Amendment makes a strong RTBF unlikely, and debates center more on consumer protection and transparency. In China, states' interest dominates, and priority is often placed on surveillance rather than privacy.

In many African jurisdictions, such as Nigeria, data protection frameworks are still developing in light of the RTBF and AI, offering avenues to learn from global debates while tailoring solutions to local contexts. These diversities underscore a major point – remedies to the friction between RTBF and AI may not admit of a universal solution, rather each jurisdiction must adapt to their technological capabilities and legal traditions.

To this end, policy responses are capable of bridging the gap between law and technology. One major approach is to interpret the RTBF not just as a literal requirement to delete data from models, but as an obligation to prevent harmful outputs. In adopting this model, the focus shifts from erasing training data to ensuring that models do not reproduce personal information in ways that harm individuals. For instance, LLMs can be filtered or fine-tuned to avoid generating sensitive information, even if the underlying training remains. This reframing aligns with the principle of data minimization under Article 5(1)(c), which can be attained through techniques such as encryption, anonymization and pseudonymization. Thus, by restricting data collection and strictly processing what is necessary, the general risk of re-identification can become structurally decreased.

Overall, a multi-pronged approach is needed to resolve this tension. Legally, the RTBF may be required to evolve into a more flexible 'right to de-link' or 'right to obscure' which would focus on limiting harmful uses of data rather than demanding impossible deletion. Thus, investment in machine unlearning, privacy-preserving design, and model accountability becomes essential as this would ensure that technological advancement does not come at the expense of human dignity.

Conclusively, it would be misguided to assume that the conflict between RTBF and AI immutability is easily resolvable. A more coherent balance lies in reframing erasure from a literal command to delete, into a practical right to suppress harmful output.

In this sense, the law's task is not to demand the impossible, but to set principled limits on how memory in AI systems can be used against individuals. With this, the challenge then would not be about erasure, but about governing AI learning in a way that preserves human dignity while sustaining technological innovation.

THE ERASURE PROBLEM: RECONCILING THE RIGHT TO BE FORGOTTEN WITH THE IMMUTABILITY OF AI MODEL TRAINING DATA

BY

KOBIMDI KELSON EMMANUEL.

1.0 INTRODUCTION

The digital era has transformed how personal data is collected, processed and remembered. At the intersection of privacy rights and Artificial Intelligence (AI) lies a challenge: the Right to Be Forgotten, which allows individuals to request deletion of their data, now confronts AI systems that embed personal data in training data in ways that make deletion nearly impossible. Unlike traditional databases that store identifiable records that can be easily removed, AI models transform vast training data into parameters that are extremely difficult to isolate and erase. This creates a tension: privacy law requires control and erasure, while AI models resist erasure. The issue extends beyond technology to legal and practical questions about balancing individual rights with the benefits of AI innovation. This essay explores that problem and offers practical recommendations on reconciling the Right to Be Forgotten with the immutability of AI model training data.

2.0 ORIGINS AND LEGAL FOUNDATION OF THE RIGHT TO BE FORGOTTEN

The Right to Be Forgotten (RTBF) emerged from the case of *Google Spain SL v Agencia Española de Protección de Datos*. In 1998, *La Vanguardia* published details of Mario Costeja González's property sale over social security debts. Years later, the resolved debts still appeared in Google search results.

Mario's complaint led to the 2014 European Court of Justice ruling, which established that search engines are "data controllers" under European Union (EU) law and must consider requests to remove links to web pages containing personal information that is inadequate, irrelevant or excessive in relation to the purposes for which they were processed.

This precedent was subsequently codified in Article 17 of the General Data Protection Regulation, 2018 (GDPR) and section 34(1)(d) of Nigeria Data Protection Act, 2023 (NDPA), and expanded beyond search engines to include all data controllers, establishing clear grounds for erasure including when personal data is no longer necessary for its original purpose, when consent is withdrawn, when data has been unlawfully processed or when erasure is required for legal compliance.

3.0 IMPLEMENTATION IN PRACTICE

The process typically involves verification of the data subject's identity, assessment of the legal grounds for erasure, balancing individual privacy rights against other legitimate interests (including freedom of expression or the data controller's compliance with a legal obligation) and technical implementation of the deletion. Data controllers must also notify any third parties who have received the data about the erasure request. In traditional digital systems, implementing the RTBF involves relatively straightforward procedures. Search engines can delist specific URLs from search results for queries. Database administrators can delete specific records or anonymize identifying information. Website operators can remove content or modify it to eliminate personal data. However, this traditional model assumes that data can be precisely located, isolated and removed without affecting other system functions. This traditional method of deletion breaks down in the context of AI model training.

4.0 How AI Models Handle Data

4.1 The Training Process: AI model training departs fundamentally from traditional data processing in that it transforms raw data into mathematical patterns embedded across the million and billions of parameters, unlike databases that store retrievable records. Training involves massive datasets, sometimes containing billions of text documents and images, which the model uses to adjust its parameters and capture patterns in the data. Large language models, including GPT-3, exemplify this transformation. GPT-3 was trained on about 570GB of text. By repeatedly predicting the next word, it developed strong language skills. The specific training data is not stored anywhere within the final model. Instead, its influence is distributed across GPT-3's 175 billion parameters.

4.2 The Immutability Problem: AI model training involves encodement of information in ways that make deletion harder than in a traditional database. In a traditional database, data can be located and removed without disturbing the rest of the database. However, in an AI model, data becomes part of the learned representations and cannot be precisely identified or extracted. This challenge is extended by the interconnected nature of neural network parameters. Each parameter is shaped by many training examples, and each training example influences many parameters. Adjusting parameters to erase one piece of data can harm performance of unrelated tasks, making precise removal nearly impossible.

4.3 Conflict Scenarios: The clash between RTBF requirements and AI immutability appears in many real-world cases. Imagine a 2015 blog post about someone's mental health struggles. Years later, now recovered, the author finds the post was used to train a large language model. Under data protection law, they can request erasure. However, the AI system cannot simply "delete" the post. It has shaped the model's understanding of mental health language, personal narratives and broader linguistic patterns. Removing this influence would mean retraining the model at great cost or using "unlearning" methods that are still experimental. Similar issues occur elsewhere.

A person whose photos were used to train facial recognition system may request removal, but those images already shaped how the system interprets features, expressions and demographics.

5.0 Legal and Regulatory Gaps and the Transparency Problem.

Current legal frameworks struggle to address these technical limitations. Section 34(1)(d) and (2) of the NDPA requires that personal data be erased "without undue delay" when certain conditions are met. However, these laws were written primarily with traditional data processing in mind and lack specific guidance for AI training scenarios. Another gap concerns the transparency principle under privacy laws. Individuals must be told how their personal data is processed, including what data was collected. This is vital because people cannot exercise the RTBF if they do not know whether their data was used in AI training. Yet, many AI companies are secretive about their training datasets, citing competition and security concerns. The EU Artificial Intelligence Act (AI Act) tries to fix this problem through its own transparency requirements.

Providers of general-purpose AI models must publish detailed summaries of their training data, including the types of data used and their sources. This requirement is a major step toward enabling meaningful RTBF enforcement in AI contexts. However, even this new transparency requirement may prove insufficient. Still, the requirement may not be enough. Public summaries give only general information, not precise details that let individuals confirm if their own data was included. In addition, AI training often involves billions of data points, making it nearly impossible for a person to find their own information. This leaves individuals filing erasure requests with incomplete knowledge, while AI companies face the challenge of responding without full visibility of their training data.

6.0 Possible Technical Solutions

6.1. Machine Unlearning: The most direct technical approach to the AI erasure problem involves machine unlearning that attempts to remove the influence of specific training data from already-trained models. This emerging field offers several promising approaches, though each comes with significant limitations and trade-offs.

6.1.1 Exact Unlearning: The aim of exact unlearning is to remove the effect of certain data points as if they were never used in training. One way to do this is to retrain the model from the beginning after removing the data. However, newer methods try to remove the data's influence without retraining the whole model, which makes the process faster and less costly. For example, the Sharded, Isolated, Sliced, and Aggregated (SISA) training method splits the model into smaller sub-models trained on different parts of the data. Making sure the data is fully removed, with no trace left in a sub-model, is especially difficult for complex models.

6.1.2 Approximate unlearning: This method tries to remove or reduce the effect of certain data points in a model, but it is less precise. Instead of retraining the whole model, updates are made to reduce the impact of the data that should be "forgotten". This can be done by changing the model's weights or adding correction factors. The goal is to weaken the data's influence enough while keeping the process fast and low-cost in terms of storage and computing. However, because this method is not exact, small traces of the data may remain, which can be risky in sensitive situations.

6.2 Data Prevention Strategies: Another way to tackle the RTFBF problem with AI systems is to ensure that data used for training does not contain personal data. There are two approaches here.

6.2.1 Prevention-focused approaches: These aim to avoid the erasure problem entirely by carefully managing what data enters AI training pipelines.

Data filtering techniques can screen training datasets to identify and exclude personal information before training begins. These methods use automated detection systems to identify personally identifiable information, private communications or other sensitive content that might later trigger erasure requests.

6.2.2 Synthetic data approach: Here, instead of training directly on real personal data, AI systems can be trained on artificially generated datasets that preserve the statistical properties of real data while containing no actual personal information. Modern synthetic data generation techniques can create highly realistic text, images, and other data types that enable effective AI training without privacy risks. However, synthetic data approaches face their own limitations. Generating high-quality synthetic data often requires training on real data initially, potentially recreating the same privacy problems. Synthetic datasets may also fail to capture important nuances present in real data, potentially leading to AI systems that perform poorly.

7.0 Suggested Legal and Regulatory Adaptations

7.1 Reasonable Forgetting: Instead of requiring complete and perfect erasure of data, legal frameworks could shift toward a standard of "reasonable forgetting" that recognizes the technical limitations of AI systems. This approach could create clear rules for when data removal is considered sufficient, even if small traces remain in the model's parameters. The rules could consider factors such as whether full erasure is technically possible, the financial and environmental costs of retraining, the sensitivity of the data involved, and the possible harm that might result if the data is retained. Regulators could gradually develop regulatory standards that balance the privacy rights of individuals with the practical limitations of technology and the wider social benefits of AI.

7.2 Sectoral Regulations: Because AI is used in very different areas, regulations may need to vary across sectors. Generally, systems that process highly sensitive personal data would normally face stricter erasure requirements to protect privacy. However, there may be exceptions where the social benefits are so significant that some flexibility is justified. However, there may be exceptions where the social benefits are so significant that some flexibility is justified. For example, medical AI systems handle highly sensitive health data, but they also have the potential to save lives. In such cases, regulators might allow less strict erasure standards if strong safeguards are in place, balancing the need for privacy with the public interest in advancing healthcare. By contrast, consumer-facing AI systems, such as recommendation engines, often pose lower social benefits while still raising privacy concerns. These systems might therefore face stricter requirements to ensure stronger protections for individuals. A risk-based approach could categorize AI systems according to both the sensitivity of the data they use and the level of social utility they provide. High-risk systems with limited social benefit would face stronger erasure obligations, while high-benefit systems could receive more flexibility, provided that privacy risks are carefully managed.

7.3 Redefining Forgetting: The technical limitations of AI suggest that society may need to rethink what "forgetting" means in this context. Instead of insisting on complete deletion of every trace of personal data, a more practical standard could focus on preventing harmful uses of data while accepting that some residual influence will remain in the model. This way of thinking matches how human memory and forgetting actually work. People rarely erase memories entirely, but laws and norms that limit how past information is used against individuals are created. For example, "spent conviction" laws in some legal systems make certain criminal convictions legally irrelevant after a set time period, even though the records still exist. If this idea is applied to AI, the focus would shift to ensuring that models cannot be used to harm individuals or target them unfairly based on personal data. Technical measures could be built into models to stop them from revealing specific personal details, while legal frameworks could prohibit using AI systems in ways that breach privacy rights.

7.4 Redefining Personal Data and the RTBF in AI Systems: A clearer and narrower definition of personal data could make the RTBF easier to apply in AI systems. At present, the broad interpretation of means that almost any data that could, even in theory, be linked to a person is treated as personal data. This makes RTBF very difficult in practice, because AI models are often trained on huge, unstructured datasets collected from the internet. Trying to delete every possible trace of a person from such datasets, and from the model itself, can be nearly impossible. The SRB v. EDPS case, which the Court of Justice of the European Union is expected to decide in September 2025, could change this. The Advocate General has already suggested that if a company cannot realistically identify someone from the data it holds, for example, because the data has been pseudonymized or aggregated so that re-identification is virtually impossible, then the data should not count as personal data for that company. If the Court accepts this view, the RTBF would apply only in situations where an AI provider can meaningfully link training data or outputs back to a specific individual. This shift would not weaken privacy rights. Instead, it would focus RTBF duties where they matter most: in cases where there is a genuine risk that personal information can be connected back to a living person. For AI developers, this would reduce impossible deletion requests while still requiring them to manage data responsibly, apply safeguards like pseudonymization, and prevent harmful uses of training data. In short, redefining personal data along the lines of the SRB case could create a more balanced and realistic way of applying the RTBF to AI.

Conclusion

The conflict between the Right to Be Forgotten and the way AI systems work presents legal and technical challenges. Since AI models learn in a distributed way, full erasure after training is almost impossible, and retraining from scratch is too costly. This does not mean privacy rights should be ignored. Instead, "forgetting" in AI should be understood in a practical way. Ideas such as reasonable forgetting, sector-specific rules, and clearer limits on what counts as personal data, which the Court of Justice may soon clarify in the SRB v. EDPS case, can help create fairer and more workable standards.

Technical methods like machine unlearning and synthetic data can reduce risks, while legal measures such as transparency rules and proportionality tests can balance privacy with social benefits. The way forward is to combine these approaches. Laws should protect privacy where risks are high, allow flexibility where public interests are strong and ensure AI developers remain accountable. Just as the first RTBF ruling found a balance for search engines, a new balance is needed for AI.

EXAMINING POLICY DEVELOPMENTS ON CROSS-BORDER DATA TRANSFERS AND DIGITAL TRADE IN NIGERIA

BY
IKENNA EMMANUEL

1.0. INTRODUCTION

In this era of 'global localization', the seamless flow of data across borders has become an indispensable catalyst for economic growth and development. Nigeria, though still a 'green' country when it comes to harnessing our digital economy, has witnessed a surge in cross-border data transfers and digital trade, thus necessitating a strong regulatory framework to safeguard both consumer privacy and facilitate innovation. This essay examines the intricate development of policies surrounding these two critical aspects in Nigeria- cross border data transfer and digital trade.

Under Nigeria's data protection regime, we will analyse the significant transformations to its policies and legislations; like the Nigerian Data Protection Act and the Data Protection Regulations, including the transition in regulatory authorities. Turning to the realm of digital trade, we will delve into the government's ambitious digital policies and highlight Nigeria's participation in the African Continental Free Trade Agreement's (AfCFTA) Digital Trade Protocol.

However, Nigeria faces a myriad of challenges when it comes to navigating the interplay between data protection, digital trade, and economic growth. Thus, we will conclude by examining the existing challenges and considerations for the future, and suggesting avenues for further development.

2.0 CROSS BORDER DATA TRANSFER

Cross-Border Data Transfers refers to the movement of data from one national jurisdiction to another, that is, data transfer between countries with different legal and regulatory frameworks.

It is not every form of data transfer between jurisdictions that constitutes cross border data transfer. It has to occur between two data management entities based in different jurisdictions, be it between two data controllers or processors.

Thus, where a Nigerian customer gives their personal information to a Chinese online shopping service, say *Alibaba,* it constitutes Data Transfer between a data subject and a controller, not between two data management entities.

In Nigeria, **the Nigeria Data Protection Act 2023**, is the main legislation governing data management and transfer.2Its objectives among other things, include: to protect the personal information of Nigerian data subjects and to establish the Nigeria Data Protection Commission. Other subsidiary legislations and guidelines include the **Nigeria Data Protection Regulations (NDPR)** and the **Implementation Framework for the Nigeria Data Protection Regulations**.

Initially, the NDPR, issued by the **National Information Technology Development Agency (NITDA)**, provided a foundational framework for data protection.4 However, it lacked legislative backing and being that it applied to only Nigerian citizens (both residents and non-residents), it could not cater for the cross border data transfer needs adequately. Under the NDPR, the enforcement powers were initially granted to the NITDA, then subsequently to another enacted agency, **the Nigerian Data Protection Bureau (NDPB)** as the capacity of NITDA was stretched thin with these overwhelming responsibilities. This move was also to concur with the provisions of the **Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data Protection**. However in both cases, these regulatory authorities exercised the powers under this legislation subject to the prerogative of the Attorney General of the Federation.8 This practice was annulled with the enactment of the NDPA; which empowers only the Nigerian Data Protection Commission to enforce the Act.

Generally, Data transfer is not permitted to other countries under the Nigerian Data Protection Act. However certain exceptions are provided and they are broadly classified under two heads; Adequacy of protection11 and other Derogations. For the former, Data Transfer by a controller would only be permitted to another country where the recipient is subject to a laws in their own country which would afford adequate protection to the personal data in their possession. What constitutes adequate protection is stipulated in Section 42 (1) & (2) of the NDPA.

The Nigerian Data Protection Commission is also empowered to issue guidelines for assessing these measures of protection and issue an adequacy decision on a country, international organisation, or sector, expressing approval or not. To this effect, a whitelist of countries has been provided under the Data Protection Implementation Framework for data controllers to consult with when entering into data transfer agreements with recipients from other countries.

Nonetheless, the Act makes other provisions for data controllers or processors to leverage on for their data transfer agreements when the recipient's country has not implemented any of the adequate protection mechanisms. Though the Act does not label these as "**derogations**," they are typically seen as a 'last minute resort' and have also been referred to this way in legal parlance due to their similarity to the derogatory provisions made in The **General Data Protection Regulations (GDPR)**.

3.0. DIGITAL TRADE

It goes without saying that Digital Trade involves buying and selling of goods and services digitally, that is, over the internet. Globally, the digital economy is now a force to be reckoned with because of its rate of expansion. The Organisation for Economic Cooperation and Development (OECD) reported that proxy measures already suggest that digital trade makes up for 25% of global trade, or just under USD 5 trillion in 2020.

This digital fever has also taken over legislation as over the past two decades, nearly one in two Regional Trade Agreements (RTA) include a digital trade provision.

The African Continental Free Trade Agreement contains amongst its provisions a Digital Trade Protocol which aims to facilitate the cross-border flow of digital products and services within the African continent. Recent OECD analysis has shown that having a digital trade chapter in a regional trade agreement can double its impact on trade.

Even the giant of Africa has not escaped this wildfire. The National Bureau of Statistics (NBS), in a 2019 report, stated that Nigeria's digital economy, contributed over 4 trillion Naira to the country's GDP. Thus, the Nigerian Government in a bid to re-orientate its oil-based Economy and integrate digital technology to restructure its economy, has aggressively introduced economic policies and channelled massive investments towards developing information and communications technology (ICT) capacity and infrastructure necessary for facilitating a digital economy.

Apart from renaming the **Federal Ministry of Communications** as the **Federal Ministry of Communications and Digital Economy**, the Nigerian government has proposed an eight-pillar **National Digital Economy Policy and Strategy** designed to harness the capacities of its agencies and properly blend them with the roles of the private sector, in building a flourishing digital economy for the benefit of Nigerians.

Another notable development in this area is the government's introduction of a novel **National Digital Economy And E-Governance Bill** this year. This legislation, though still under deliberation, aims to create a comprehensive legal framework for digital transactions, addressing issues such as electronic signatures, e-commerce contracts, and online dispute resolution. The passage of this Bill would provide a much-needed boost to digital trade in Nigeria, offering greater legal certainty and protection for businesses and consumers alike.

Moreover, Nigeria being a signatory to the African Continental Free Trade Agreement (AfCFTA), has actively participated in the implementation of its Digital Trade Protocol which has presented significant opportunities for digital trade in the country.

4.0. Challenges and Considerations
Despite these positive developments, Nigeria faces several challenges and must consider various factors in its pursuit of a thriving digital trade ecosystem:

4.1. Infrastructure Gap:
Many regions within the country still lack adequate broadband connectivity, limiting access to digital services and hindering the efficient transfer of data. Nigeria has been persistently ranked as one of the countries with the lowest broadband penetration (37.86%) in the world. Addressing this infrastructure gap is essential for creating a conducive environment for digital commerce.

4.2. Regulatory Harmonization:
The proliferation of digital technologies and the increasing interconnectedness of the global economy necessitate a harmonized regulatory framework for cross-border data transfers and digital trade.

However, Nigeria is recognised as one of the emerging world economies with the strictest requirement for data localisation restricting the flow of data across borders. Yet, she is a signatory to many regional and international agreements. While these Data Protection laws are put in place to ensure the protection of her citizens' digital rights and security of the data, it does not help our developing economy as it discourages tech investors and companies. It is my opinion that these strict measures be relaxed.

4.3. Digital Literacy:
Enhancing digital literacy among the population is vital for promoting the adoption of digital technologies and participating effectively in the digital economy. By equipping individuals with the skills necessary to navigate the digital world, Nigeria can empower its citizens and foster a more inclusive digital society.

5.0. Conclusion
Nigeria's journey towards a thriving digital economy is inextricably linked to its ability to navigate the complex landscape of cross-border data transfers and digital trade. While significant progress has been made through the NDPA and the introduction of many digital trade policies, several challenges remain. To fully realize its potential, Nigeria must prioritize infrastructure development, regulatory harmonization, data privacy protection, digital literacy, and international cooperation.

Then and only then, can Nigeria create a conducive environment for innovation, economic growth, and the protection of its citizens' rights in the digital age.

EXAMINING POLICY DEVELOPMENTS ON CROSS-BORDER DATA TRANSFERS AND DIGITAL TRADE IN NIGERIA

By
ENOCH AKINBUSOYE AKINLABI

1.0 INTRODUCTION

Data is the lifeblood of the digital economy and the primary protagonist in the prodigious tale woven by the digital era. The digital universe comprises about 44 zettabytes of data, which amounts to 40 times the number of stars in the known universe! It is therefore unsurprising that data is considered especially important due to its multifarious roles in the 21st century, including but not limited to aiding decision-making, analysis, troubleshooting, transformation and innovation.

The internet has significantly transformed how goods and services are bought, sold, and delivered internationally and domestically. Digital trade comprises *inter alia* e-commerce, fintech services, software exports, and cloud services. The digital economy in Nigeria has seen rapid expansion, mirrored by the increase of internet users from 97 million to 107 million between 2017 and early 2025, with penetration reaching 45.4 percent. The sector's contribution to GDP peaked at 19.78 percent in Q2 2024, underscoring its growing economic weight. Alongside this expansion of digitally enabled trade is naturally the increase in cross-border data flows to provide access to the global digital ecosystem.

Cross-border data transfer involves the sharing of personal data across different jurisdictions. Though it comes with a slew of attendant consequences, it is essential in digital trade as the latter is inherently cross-sectoral and multi-dimensional. As the digital era progresses, it becomes increasingly important to have clear policies as regards digital trade and the cross-border transfer of data. Doubly so for Nigeria, a regional tech hub and one of the largest economies in Africa.

In light of this, this essay examines recent policy developments in this regime, highlights obstacles and tenders recommendations to create an enabling environment for digital trade in Nigeria.

2.0 Policy Developments in Nigeria

The interconnected nature of cross-border data transfers and digital trade has resulted in some overlap in the policies addressing them:

2.1 Nigeria Data Protection Act (NDPA) 2023

The Act enacted on June 12, 2023, builds on provisions of the erstwhile Nigeria Data Protection Regulations (NDPR) 2019 and its Implementation Framework. Section 1 firmly states its objective is to safeguard the rights and freedoms of data subjects guaranteed under the Constitution. Section 2 of the NDPA further widens its scope of operation as compared to Paragraph 1.2 of the NDPR. Sections 41 to 43 of the NDPA set out the basis for the cross-border transfer of personal data. Primarily the Act prohibits data transfers unless the recipient is subject to laws that provide an adequate level of protection, or the transfer falls within the acceptable exceptions set out in the Act. The NDPR and its Implementation Framework remain relevant per Section 64(2)(f) of the NDPA, but the latter takes priority under Section 63. The Nigeria Data Protection Commission (NDPC) has also replaced the Nigeria Data Protection Bureau and taken over its functions.

A significant update came in 2025 with the issuance of the NDPA General Application and Implementation Directive (GAID) by the NDPC on March 20, 2025, which officially took effect on September 19, 2025, after a six-month transition period. The GAID operationalizes the NDPA, replacing the NDPR with detailed compliance guidelines, including enhanced provisions for cross-border transfers. It specifies two primary legal bases: adequacy decisions and appropriate safeguards. Alongside exceptions like explicit consent or contractual necessity, while introducing requirements for Data Protection Compliance Organisations (DPCOs) to assist businesses.

Additionally, in August 2025, the NDPC issued compliance notices to data controllers and processors, mandating detailed reporting within 21 days to bolster enforcement.

2.2 AfCFTA Protocol on Digital Trade

This protocol aims to drive the expansion of digital trade within the African continent amongst 1.3 billion people in a single trade area with a combined estimated GDP of $3.4 trillion. It subsists within the wider framework of the African Continental Free Trade Agreement, to which Nigeria is a signatory. It addresses pertinent issues in data protection, data governance and cross-border data flows. Articles 20 and 22 promote a default rule of free flow of data and generally lean towards creating a unified" digital market. Adopting this Protocol is envisaged to bolster Nigeria's exports by 16.9% to 59.8% and increase its GDP by approximately 11.7% to 12.8%.

Since the protocol's adoption in February 2024, progress has accelerated in 2025. The eight annexes were finalized in February 2025, paving the way for ratification. Nigeria, the AfCFTA Digital Trade Champion, hosted its inaugural AfCFTA Digital Trade Protocol Hackathon in Lagos from May 1st to 3rd, 2025 fostering innovations in e-commerce, payments, and logistics to align with the protocol's goals. While full ratification remains pending, these steps position Nigeria to leverage the protocol for enhanced digital trade integration.

2.3 Other National Policies

Other relevant national policies include the following; the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) (as amended, 2019), Guidelines on Point of Sale (POS) Card Acceptance Services 2011, the National Digital Economy Policy and Strategy (NDEPS) 2020-2030, the 2021 National Policy for the Promotion of Indigenous Content in the Nigerian Telecommunications Sector, the Nigerian National Broadband Plan 2020–2025, the 2012 National Financial Inclusion Strategy, the Nigeria Cloud Computing Policy 2019, and the National Cybersecurity Policy and Strategy (NCPS) 2021. Section 64 of the NDPA titled 'Transitional Provisions' saves the operation of a number of these guidelines.

Recent advancements include the Ministry of Communications, Innovation, and Digital Economy's announcement of a broadband enhancement project to boost connectivity. In 2025, the Nigerian Communications Commission (NCC) proposed a spectrum strategy to support broadband expansion and space services, aligning with national goals for rural connectivity.

Additionally, Nigeria joined the Digital Public Goods Alliance in October 2025 to advance open digital transformation through initiatives like the 3MTT program.

2.4 Other International Policies

Aside from the AfCFTA, Nigeria draws inspiration from other regional and international frameworks, including the UNCITRAL Model Law on Electronic Records (MLETR) 2017, and the 2010 ECOWAS Supplementary Act on Personal Data Protection. Interestingly, Paragraph 16 of the NDPR's Implementation Framework allows recourse to be made to the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014 and the EU's General Data Protection Regulation where there is a lacuna. Nigeria is also a part of the WTO's Joint Statement Initiative (JSI) on Electronic Commerce. In 2025, Nigeria's engagement in WTO-led digital trade initiatives continued to emphasize fast-tracking growth amid global commitments.

3.0 Stumbling Blocks to Progress

3.1 Balancing Competing Policy Goals: Nigeria like any other country struggles to juggle maintaining digital sovereignty and allowing cross-border data flows, with economic (potential benefit and cost) and non-economic (communication surveillance and data security) justifications for both stances. As a result, Nigeria suffers from high regulatory fragmentation and is considered the second most restrictive nation in Africa when it comes to digital trade. The GAID 2025's stringent cross-border rules, while enhancing protection, have amplified concerns over compliance burdens for businesses.

3.2 Digital Illiteracy and Regulatory Delay: The Wiley Digital Skills Gap Index ranks Nigeria 11th in Africa and 103rd globally. This knowledge gap is unacceptable given the fast-moving pace of the digital age. Unfortunately, Nigeria also has a track record of legislative gridlock which affects the ability of laws to reflect rapidly changing realities in the digital space. While the GAID 2025 addresses some ambiguities, delays in full enforcement persist.

3.3 Cybersecurity and Data Protection: Robust frameworks that address cybersecurity, digital sovereignty and data privacy are a must for digital trade and seamless cross-border data transfer. Although Nigeria has made strides in this area, enforcement and implementation remain a thorny issue. The Cybercrimes (Prohibition, Prevention, Etc) (Amendment) Act 2024, enacted to tackle evolving threats, underscores ongoing vulnerabilities.

3.4 National and Supranational Harmonisation: Lack of effective coordination between various national regulatory bodies pursuing different goals is a major challenge in this area. Not to mention the divergence between Nigeria's restrictive cross-border data policies and its commitments under the AfCFTA and other international agreements. Recent WTO and World Bank warnings in October 2025 highlight how regulatory gaps could hinder Nigeria's digital trade gains.

3.5 Ambiguity and Infrastructure Deficit: Several ambiguities are present in the NDPA. For example, the Act fails to elucidate pertinent phrases like 'data controller and data processor of major importance', 'legitimate interest' as a lawful basis for processing data, and 'persons incapable of giving consent'. The GAID 2025 has begun clarifying these, including through DPCO requirements, but implementation remains to be seen.
Moreover, gaps in the digital infrastructure needed to ensure compliance still abound. Secure data centres and high-speed internet remain unavailable in many parts of Nigeria with 40% of the population without access to the internet and 55% of rural areas without access to power. Weak broadband infrastructure poses a risk of exclusion from continental digital trade opportunities, as noted in recent analyses.

4.0 Recommendations
4.1 Clarification of National Policies and Inter-ministerial Synergy: There is a need for clearer elaboration as regards contentious matters in Nigeria's national policies towards digital trade and cross-border data transfers. In this regard, the NDPA General Application and Implementation Directive (GAID) was a step in the right direction; now formally issued and effective since September, 2025, it provides a stronger foundation, though further guidance on emerging issues like AI in data processing is warranted. We also need to foster inter-ministerial collaboration to promote a straightforward decision-making process and avoid duplication of function, otherwise regulations will lose their efficacy.

4.2 Harmonisation and Regulatory Convergence: If Nigeria is truly to benefit from its international and regional agreements, a reform of its national regulatory outlook to reflect its commitments under these agreements is needed. This in no way proposes jettisoning our national stance, instead, we need to create a broad-based cross-border data transfer and digital trade policy that balances the country's regulatory objectives and our international commitments while reflecting international best practices. Aligning with the AfCFTA implementation efforts, such as the 2025 hackathon outcomes, could accelerate this.

4.3 Invest in Digital Infrastructure: To maximize the benefits from the recent policy developments Nigeria needs to prioritise investment in digital infrastructure and human capital. This will further improve the environment for innovation and facilitate greater investment in digital trade in Nigeria. The NCC's 2025 spectrum strategy offers a promising avenue, but urgent funding for rural broadband is essential to mitigate exclusion risks.

4.4 Promote Digital Literacy and Awareness: Chances to upskill digital skills and information on salient policies of digital trade and cross-border data transfer need to be made readily available to the populace to ensure successful implementation of these policies.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*
[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*
[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*
[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

The Three Million Technical Talent (3MTT) digital literacy initiative launched by the Federal Ministry of Communication, Innovation and Digital Economy (FMCIDE) and the National Information Technology Development Agency (NITDA) in 2023 is a good example of such an initiative. And its expansion through the Digital Public Goods Alliance membership in October 2025 could enhance its impact.

4.5 Expand Enforcement Capacity: Robust frameworks with insufficient enforcement mechanisms amount to a bark with no bite. Nigeria needs to enhance the capacity of relevant regulatory bodies to enforce the policies that have been put in place regarding cross-border data transfers and digital trade. The NDPC's 2025 compliance notices represents progress, but scaling resources for audits and penalties will be crucial.

5.0 Conclusion

"If you want to go fast, go alone. If you want to go far, go together." This is reminiscent of the fact that with government commitment and strong stakeholder participation, a resilient and workable ecosystem for burgeoning digital trade is feasible in Nigeria. Though obstacles like infrastructure deficits and regulatory harmonization persist, the issuance of GAID 2025, AfCFTA implementation strides, and initiatives like the broadband project position Nigeria to unlock the full potential of its digital economy within the wider scope of the continent's digital economy which is projected to reach $180 billion by 2025, by leveraging the aforementioned recommendations. Only through this, will we be able to strike the delicate balance needed between data protection and facilitating cross-border data flows towards improved digital trade.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

EXAMINING POLICY DEVELOPMENTS ON CROSS-BORDER DATA TRANSFERS AND DIGITAL TRADE IN NIGERIA

By
EDUN OLUWATOYIN

Introduction

In today's digital world, data has emerged as a crucial asset often referred to as "the new oil" that propels businesses and industries forward. It serves as a foundation for targeted advertising, enhanced services and valuable insights into consumer behavior. As data analytics becomes increasingly integral to business operations, it is essential for organizations to comprehend the regulatory framework governing data usage. This is particularly important for both local and multinational companies operating in the Nigerian market, as they must navigate the requirements of Nigerian data protection laws concerning cross-border transactions. However, the collection, storage and processing of personal data carry significant risks to individual's privacy and security, especially when such data is transferred internationally. This data often includes sensitive information such as financial details, health records and personal identifiers, which if compromised, can result in identity theft, fraud and various forms of cybercrime.

To address these issues, the European Union (EU) implemented the General Data Protection Regulation (GDPR) in 2018, establishing stringent rules for data processing within the EU and the transfer of personal data outside its borders. The introduction of the GDPR marked a significant shift in data protection regulations, imposing hefty fines on companies that fail to comply. A notable example is the record fine of $1.3 billion levied against Meta, the parent company of Facebook, by the Court of Justice of the European Union (CJEU). The CJEU determined that Meta's arrangements did not adequately mitigate the risks to the fundamental rights and freedoms of data subjects. This ruling ultimately led to the imposition of the fine for violations of privacy laws.

In Nigeria, the recently enacted Nigeria Data Protection Act (NDPA) 2023 governs the processing of personal data. It regulates the privacy rights of data subjects in Nigeria. The law applies to any organization that processes personal data of individuals in Nigeria, regardless of the organization's location. This includes data controllers and processors that are domiciled, ordinarily resident or operating in Nigeria.

Digital trade in Nigeria is experiencing significant growth, fueled by increased internet access and a youthful population eager for online commerce. The National Bureau of Statistics reported that Nigeria's digital economy contributed about 17% to the GDP in 2020, underscoring its role in economic development. As Nigeria aims to lead in Africa's digital landscape, effective regulation of digital trade is essential, particularly regarding cross-border data transfers. However in this piece, I will be discussing the policy developments surrounding cross-border data transfer and digital trade in Nigeria.

Keywords: Policy development, cross-border data transfer and digital trade.

To begin with, what is cross-border data transfer? As defined by the Nigeria Data Protection Regulation (NDPR) 2019, involves transferring personal data outside Nigeria to another sovereign state. The NDPR and its Implementation Framework govern these transfers, ensuring that any personal information identifying a Nigerian citizen is regulated and subject to restrictions. For instance, if a Nigerian company (Company A) processes employee data and collaborates with a foreign company (Company B) for HR services, this constitutes a cross-border data transfer. Also, companies must establish data transfer agreements with foreign entities, outlining the terms and protective measures for personal data. Countries with adequate data protection laws are included on a whitelist in the NDPR framework.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

While the Nigeria Data Protection Act 2023 (NDPA) aims to strengthen regulations on cross-border transfers, gaps remain in sections 42-44, which depend on the adequacy of the receiving country's laws. The NDPA does not repeal the NDPR but adopts its provisions, including the requirement for Attorney General approval for transfer requests. If no adequacy decision exists, transfers must meet specific conditions, such as obtaining consent from the data subject or transferring data for contractual obligations or legal claims.

According to the European Union, digital trade refers to commerce facilitated by electronic means, including telecommunications and ICT services, and encompasses the trade of both goods and services. This broad category includes various activities such as e-commerce, online services, and the cross-border transfer of data.

Flowing from the above, Nigeria has made significant progress in developing policies that support digital trade. The National Digital Economy Policy and Strategy (NDEPS) launched in 2020, articulates the government's vision for a digital economy that promotes innovation, entrepreneurship and job creation. It underscores the necessity of fostering a conducive environment for digital businesses and enhancing digital infrastructure. However, Nigeria's approach to digital trade is influenced by several key laws and regulations.

The Nigeria Data Protection Regulation (NDPR) enacted in 2019, aims to safeguard individual privacy and regulate the processing of personal data. It establishes guidelines for data collection, storage and transfer, ensuring that businesses adhere to data protection standards.

Another policy development is that, the National Digital Economy and E-Governance Bill, 2024, represents a strategic advancement in Nigeria's digital transformation journey. This Bill is designed to stimulate economic growth through digital technology, enhance public service delivery, and foster a competitive environment for the Nigerian digital economy. It also aims to develop export-oriented capacities within Nigeria's digital sector, support international digital trade and investments and provide a legal framework for these activities.

Notably, the Bill includes provisions that set guidelines for the operation of e-commerce platforms in Nigeria. Instructively, section 39 specifically addresses the information requirements for all e-commerce platforms, meaning that if the Bill is enacted, major platforms like Jumia and Konga, as well as smaller industry players, will face more stringent regulations. This could lead to the introduction of new taxes and levies by the National Information Technology Development Agency (NITDA) and e-commerce platforms may incur fines for violating any provisions of the law relevant to their operations.

Furthermore, these initiatives align closely with Nigeria's broader ambitions in the digital realm, particularly regarding regional integration through the Digital Trade Protocol of the African Continental Free Trade Area (AfCFTA). This Protocol aims to streamline digital trade across African nations by removing barriers and harmonizing policies to facilitate cross-border e-commerce and digital transactions.

Together, these efforts create a framework that not only enhances Nigeria's digital infrastructure and public services but also positions the country as a key player in the African digital economy, providing opportunities to expand its digital market and enhance regional trade.

Nevertheless, several challenges impede the growth of digital trade in Nigeria. The absence of a cohesive legal framework creates uncertainty for businesses. As the digital trade expands, so do the associated risks of cyber threats and implementing robust cybersecurity measures is essential for building trust among consumers and businesses engaged in online transactions. Thus the importance of the Cybercrime Act of 2015, which addresses cybercrime and establishes a legal framework for combating online fraud, identity theft, and other cyber-related offenses.
Despite this challenge, Nigeria's digital trade landscape is filled with opportunities. The increasing adoption of mobile technology and the growth of e-commerce platforms present significant avenues for businesses to access new markets.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

Conclusion and Recommendations

In the final analysis, with millions of data transactions occurring globally each day, it is imperative for Nigeria to establish a robust data protection framework for cross-border data transfers. Compliance with Nigerian laws regarding data transfer is essential for companies to avoid significant financial penalties from the National Information Technology Development Agency (NITDA), as demonstrated by the Meta case.

It is worthy of note that both local and foreign companies handling the data of over 1,000 Nigerian citizens must engage the services of a licensed Data Protection Compliance Organization. This engagement is crucial for reviewing their data handling practices and ensuring adherence to compliance standards despite existing conflicts in the regulations governing data protection in Nigeria, organizations are strongly encouraged to strictly comply with the provisions of the Nigeria Data Protection Act (NDPA) and the Nigeria Data Protection Regulation (NDPR). Companies should also proactively collaborate with the Nigeria Data Protection Commission, particularly concerning cross-border data transfers

Notably, the Bill includes provisions that set guidelines for the operation of e-commerce platforms in Nigeria. Instructively, section 39 specifically addresses the information requirements for all e-commerce platforms, meaning that if the Bill is enacted, major platforms like Jumia and Konga, as well as smaller industry players, will face more stringent regulations. This could lead to the introduction of new taxes and levies by the National Information Technology Development Agency (NITDA) and e-commerce platforms may incur fines for violating any provisions of the law relevant to their operations.

Furthermore, these initiatives align closely with Nigeria's broader ambitions in the digital realm, particularly regarding regional integration through the Digital Trade Protocol of the African Continental Free Trade Area (AfCFTA). This Protocol aims to streamline digital trade across African nations by removing barriers and harmonizing policies to facilitate cross-border e-commerce and digital transactions.

Together, these efforts create a framework that not only enhances Nigeria's digital infrastructure and public services but also positions the country as a key player in the African digital economy, providing opportunities to expand its digital market and enhance regional trade.

Nevertheless, several challenges impede the growth of digital trade in Nigeria. The absence of a cohesive legal framework creates uncertainty for businesses. As the digital trade expands, so do the associated risks of cyber threats and implementing robust cybersecurity measures is essential for building trust among consumers and businesses engaged in online transactions. Thus the importance of the Cybercrime Act of 2015, which addresses cybercrime and establishes a legal framework for combating online fraud, identity theft, and other cyber-related offenses.

Despite this challenge, Nigeria's digital trade landscape is filled with opportunities. The increasing adoption of mobile technology and the growth of e-commerce platforms present significant avenues for businesses to access new markets.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

REPOSITIONING DATA PROTECTION AUTHORITIES IN THE ERA OF ARTIFICIAL INTELLIGENCE: NIGERIA AS A CASE STUDY

BY

OLUFOLAJIMI OTITOOLA

INTRODUCTION

Artificial Intelligence (AI) is no longer a futuristic concept confined to sci-fi movies—it's here, continuously being integrated into our daily lives. With Nigeria's fast-growing tech scene and large population, the country is emerging as a fertile ground for AI innovations, spanning sectors like healthcare, agriculture, manufacturing, finance, retail, education, and law. The Nigerian Government has also taken steps to harness of AI for sustainable development to foster innovation, productivity, and human welfare. AI presents novel opportunities for innovation and tackling inefficiencies in several sectors of the Nigerian economy. However, AI presents unprecedented challenges, particularly in safeguarding data privacy and protection.

At the centre of data protection are Data Protection Authorities (DPAs), whose primary roles include investigation, ensuring compliance, and enforcement of regulations. As AI technologies evolve, DPAs must adapt to address the unique privacy risks these innovations present. This essay examines how Nigeria's DPA, the Nigeria Data Protection Commission (NDPC), can reposition itself to regulate AI effectively, safeguard data subjects' rights, mitigate potential risks, and draws insights from global regulatory frameworks to build a robust and forward-looking governance structure.

2.0 CONCEPTUAL BACKGROUND

Adopting a universal definition for "AI" has proven difficult, as various stakeholders approach the concept from different perspectives. AI encompasses a range of technologies, such as robotics, automation, and machine learning, that exhibit aspects of human intelligence and operate autonomously.

Given this diversity, no single definition fully captures the breadth of AI systems. Rather than attempt to create a single, all-encompassing definition, a more practical approach is to define AI contextually, based on the specific tasks the system performs. This method recognizes the diversity of AI applications and makes the concept more accessible to a broader audience. For the purpose of this essay, AI can be understood as intelligent systems designed to "think" and "act" like humans, with varying levels of human intervention depending on the application. This simplified conceptual background provides a foundation for discussing AI without getting bogged down in complex technical definitions, while still acknowledging the breadth and adaptability of AI technologies.

3.0 PRIVACY AND DATA PROTECTION CONCERNS ASSOCIATED WITH AI VIZ-A-VIZ THE NIGERIAN DATA PROTECTION REGIME

The deployment of AI systems in Nigeria raises significant privacy and data protection concerns. The lifecycle of AI—from development (machine learning) to deployment—introduces points of vulnerability where regulatory oversight is essential to prevent misuse or violations of privacy rights.

3.1 AI Development Stage

The AI development stage, from ideation to testing, involves the collection, processing, and use of large volumes of data to train AI models. Key privacy and data protection concerns arise during this stage.

First, the legal basis for data collection as AI developers must ensure that personal data is collected lawfully. Improper data collection (e.g., through web scraping) during development without appropriate and justifiable legal basis can lead to unlawful data processing violating the NDPA and NDPR. Also, if the purpose for data processing changes, the initial legal basis at the commencement of the processing activity may become inadequate.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

Second, data quality is important because the personal data used for AI training must be accurate and fit for purpose. Biased or inaccurate data can result in discriminatory outcomes. This has been noted in the United States, where AI-drive (predictive) policing has led to biased results due to flawed data used for training. The NDPR and NDPA emphasise the need for accurate and adequate data processing to prevent biased results.

Lastly, another concern is AI systems that collect excessive. For example, Large Language Models (LLMs) and AI systems with automatic speech recognition tend to capture vast amounts of personal data. The NDPA and NDPR uphold the data minimisation principle, requiring that only the necessary personal data be processed for a specific purpose. The large-scale data collection by AI systems may breach this principle.

3.2 AI Deployment Stage

The AI deployment phase, where AI products are launched, presents significant data protection concerns, including transparency, data security, purpose limitation, and automated decisions.

The principle of transparency, which requires data subjects to be provided with information about the life cycle of the data protection activity, affects the development and deployment stages. The complexity of AI systems, often described as "black-boxes," can obscure their functionality, making it difficult for data subjects to understand how their data is processed. The lack of transparency undermines trust and accountability. The NDPR requires clear and accessible information about data processing, which is echoed in the NDPA's explicit transparency obligations.

Regarding data security, AI relies on multiple networks to function, increasing data security risks, particularly in cross-border data transfers and Internet of Things (IoT) setups. The NDPR and NDPA mandate technical and organisational measures to protect data, but AI's complexity introduces challenges such as data tampering and insider threats.

Furthermore, AI systems must be deployed with clearly defined purposes for data processing. If AI systems operate without maintaining these purposes throughout their lifecycle, they risk violating the principle of purpose limitation. NDPR and NDPA emphasise purpose limitation principle and the importance of safeguarding against data repurposing. If AI systems are employed without clearly identifying their purposes at the outset of the processing activity or maintaining those purposes throughout the AI life cycle, it can violate the principle of purpose limitation. For example, personal data collected for one purpose might be repurposed for AI training without the knowledge or consent of the data subjects.

In addition, AI-driven automated decision-making systems (e.g., in credit scoring, healthcare, etc.) can affect data subjects' rights by making significant decisions without human intervention. These systems rely on algorithms trained on data, which may carry inherent biases or errors. In healthcare, AI systems can make decisions based on data patterns, which may lead to biased or incorrect outcomes if the training data is flawed. This could result in disproportionate treatment recommendations or denial of care for certain groups based on flawed patterns or assumptions. Without human oversight, such errors may go unchecked, negatively impacting patient care. Section 37 of the NDPA grants data subjects the right to avoid decisions based solely on automated processing, with measures allowing for human intervention and contesting decisions, addressing concerns about AI's error margin and lack of transparency.

Given the privacy risks posed by AI, maintaining operational compliance is key. Organizations developing or deploying AI systems must keep detailed records of their processing activities and conduct Data Protection Impact Assessments (DPIAs) as required by Section 28 of the NDPA. DPIAs help assess potential risks associated with AI-driven data processing and ensure that appropriate measures are in place to protect individuals' rights.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

4.0 The Current Activities of the NDPC in Data Protection in Nigeria

The current framework established by the NDPA and NDPR serves as a foundational starting point for data protection enforcement regarding AI in Nigeria. By outlining essential principles and obligations for data controllers and processors, the NDPC is positioned to implement and promote compliance across various sectors.

Since its establishment in 2022, the NDPC, a shortstaffed and underfunded organisation, has leveraged multistakeholder partnerships to carry out its responsibilities. Notably, it has engaged licenced data protection compliance organisations (DPCOs) from the private sector as key partners in monitoring data compliance. These DPCOs conduct data audits, impact assessments, data privacy trainings, and liaise with the NDPC, allowing the NDPC act to maintain a supervisory role in targeted data privacy and protection compliance investigations.

Additionally, the NDPC issued the General Application and Implementation Directive (GAID) 2024, which covers different areas of data protection, including AI and IoT. Particularly, article 44 of the GAID provides that a data controller or processor who deploys or intends to deploy emerging technologies, such as AI, must consider the NDPA, public policy, the GAID and other NDPC instruments.

However, despite these efforts within its short establishment period and with limited resources, the NDPC currently faces significant challenges in effectively managing the complexities of data protection in the AI era.

Repositioning the NDPC in the Era of AI

Section 5 of the NDPA empowers the NDPC with responsibilities, including regulating the deployment of technological measures to enhance personal data protection, investigating data privacy violations, collaborating with other ministries and agencies, and initiating legal actions. The NDPA encompasses all forms of personal data processing, including data utilised in AI systems. These provisions as the foundation for the NDPC to monitor and enforce data protection compliance within the AI sector, provided they are effectively utilised.

It is recommended that the NDPC establishes a GAID specifically for emerging technologies like AI, IOTs, and blockchain. The GAID should mandate continuous DPIAs throughout the various stages of AI systems that process personal data. The GAID should also develop a standardised framework for conducting DPIAs, focusing on potential risks that come with AI systems and their impact on individuals' rights. In addition, the GAID should establish procedures for user-friendly reporting mechanisms that enable individuals to report AI-related data breaches or misuse of personal data. Given the likelihood of frequent reports, the NDPC could implement a tiered approach for redress, partnering with DPCOs or relevant sector regulators where AI system are deployed.

Immediate steps are needed to enhance public awareness and capacity building for monitoring compliance. A November 2023 survey revealed that 41% of respondents indicated an average level of public awareness of data protection, while 29% reported below-average awareness. Awareness has been identified as a priority the NDPC must address to improve compliance with the NDPA. It is crucial that data subjects are informed of their rights. The use of mass media and social media for public awareness campaigns, including FAQs, fast facts, and short notes on personal data rights and the role of DPCOs, will help increase understanding and compliance.

Currently, there are 163 licensed DPCOs serve as the foot soldiers of the NDPC, monitoring data protection compliance. However, the scale of the task ahead for data protection compliance is immense. According to the NDPC Nigeria Data Protection Annual Report 2023, over 500,000 data controllers and processors are targeted for registration, but compliance levels remain low. In 2023, fewer than 2,000 companies filed data audits, representing a significant gap in enforcement and oversight. To bridge this gap, the NDPC must take immediate steps towards capacity building, including expanding the network of DPCOs.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

Additionally, there is need for cross-sector partnership with other governmental agencies to ensure consistent efforts across sectors. For example, the CBN recently emphasised the importance of proper KYC protocols for its regulated entities. Given the large volume of customers, digital verification of identities and other KYC information may be done. It is important to ensure that data protection principles and rights of data subjects are upheld. Similarly, where AI impacts on labour rights–such as in recruitment processes or employee performance evaluations–the NDPC could partner with the Federal Ministry of Labour and Employment to address any data protection concerns.

Furthermore, the NDPC is currently not actively involved in relevant discussions regarding the development of national AI policies and strategies. The current draft National AI Strategy issued in August 2024 is filled with avoidable misnomers, misconception regarding the NDPA's scope, and lack of recognition of the NDPC's role in AI research, development, and deployment. This contrasts the EU's approach, where DPAs play a central role, as market surveillance authorities, in enforcing the AI Act and the GDPR.

Lastly, given the cross-border nature of AI systems, international collaboration is key. Nigeria is yet to ratify the African Union Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention), which in Article 28 emphasises international cooperation and exchange of information between State Parties. Also, Nigeria, while a member of the Global Privacy Assembly—an organisation of over 130 DPAs cooperating on the adequacy of data protection across jurisdictions—needs to enter into bilateral agreements with countries where Nigerian citizens' data frequently crosses borders.

Such partnerships will enhance Nigeria's data protection landscape and ensure compliance with global standards.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

REPOSITIONING DATA PROTECTION AUTHORITIES IN THE ERA OF ARTIFICIAL INTELLIGENCE: NIGERIA AS A CASE STUDY

By
RAHAMAT

Nigeria is currently witnessing significant advancements in artificial intelligence (AI), as both government and private organizations strive to leverage this technology for economic growth. A research survey conducted in January 2025 by Ipsos, in collaboration with Google, found that 70% of the online population in Nigeria has utilized generative artificial intelligence. This statistic indicates that Nigeria's AI adoption rate surpasses the global average. However, the advancement of AI in the Fourth Industrial Revolution raises critical issues concerning privacy and data protection. These concerns are particularly pressing in sub-Saharan African countries, such as Nigeria, where public understanding of data privacy remains limited.

While Europe has taken the lead by enacting the European Union AI Act, many countries are relying on existing legislation, such as Data Protection Acts, to tackle challenges posed by AI, including privacy erosion, algorithmic bias, and human rights infringements. Data Protection Authorities (DPAs) are increasingly positioned as frontline defenders in AI reforms. This essay discusses the current role of the Nigeria Data Protection Commission ('NDPC' or 'The Commission') in addressing privacy and human rights concerns related to AI deployment in Nigeria and recommends practical approaches the Commission should take to reposition itself in the AI Era.

CONTEXT OF DATA PROTECTION IN NIGERIA

Nigeria's data protection landscape continues to evolve. The need for a formal legislative framework to govern data protection in Nigeria emerged from rapid technological advancements and large-scale data processing activities, which necessitated institutional measures to protect the personal data of Nigerian citizens and residents.

The primary legislation governing this ecosystem is the Nigeria Data Protection Act (NDPA) 2023, complemented by the General Application and Implementation Directive (GAID) 2025. The NDPA is modeled significantly after the EU General Data Protection Regulation (GDPR).

In addition to the NDPA and GAID, other Nigerian laws such as the Freedom of Information Act, the NITDA Act, the Nigeria Police Act, the Federal Competition and Consumer Protection Act, the Cybercrimes (Prohibition, Prevention, etc.) Act, and the Child Rights Act also impact privacy and data protection. The Nigerian government has prioritized AI in recent policies, exemplified by the establishment of the National Centre for AI and Robotics (NCAIR) in 2020, and the development of a National AI Strategy in 2024. Soft laws like the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, the NDPC Strategic Roadmap and Action Plan (SRAP), and the NDPA General Application and Implementation Directive (GAID) also refer to Artificial intelligence. The government aims to transform the Nigerian digital economy through these tools by promoting research and development in emerging technologies.

The data protection authority ('DPA', also known as supervisory authority) is the recognized public body empowered to perform supervisory functions in the field of privacy including monitoring, advising, investigating, suing, hearing claims, and prescribing penalties or enforcement actions amongst others. The Nigeria Data Protection Bureau (NDPB) was created in 2022 to oversee the implementation of the Nigeria Data Protection Regulation (NDPR) 2019. Following the enactment of the Nigeria Data Protection Act (NDPA) in 2023, the Nigeria Data Protection Bureau became the Nigeria Data Protection Commission (NDPC). The NDPC aims to establish a sustainable and trusted ecosystem for data protection and privacy by 2027. This laudable goal cannot be achieved without institutionalizing regulatory frameworks and policies to address the data privacy challenges of Artificial Intelligence in the 4th Industrial Revolution.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

IMPACT OF AI ON DATA PROTECTION

AI may be defined as the application of higher computing powers, data, and analytics to existing technologies to produce extraordinary results.

Assessing the impact of AI on data protection is crucial for understanding the role of DPAs in regulating privacy issues. The challenges posed by AI are not entirely new, rather, they represent an evolution of existing privacy concerns that have been exacerbated by technological advancements.

AI introduces new complexities and dimensions to problems of commercialization, weaponization, and misuse of personal data, bringing about a heightened awareness. The extensive collection and processing of personal data by AI systems raise serious concerns about privacy violations and the misuse of sensitive information. AI's reliance on vast amounts of data (often obtained through web scraping) conflicts with individual privacy rights and undermines foundational principles like fairness and transparency. AI outputs may violate privacy rights through the production of incorrect information about individuals. Machine Learning algorithms are capable of making (sometimes erroneous) inferences about people based on their training data, even when they've been trained with non-personal or anonymized data.

The NDPA and the GAID supplemented by whitepapers, strategies, and directives that make up the current framework for privacy regulations in Nigeria can address some aspects of AI-related challenges to an extent, however, the nuances of the challenges posed by AI cannot be fully encompassed by existing legislations alone. Although it may be argued that Nigeria should follow Europe's lead by enacting an AI-specific law, such legislative changes are likely to take time due to Nigeria's complex law-making process. It took 14 years for the NDPA to be enacted after its initial proposal in 2010. Therefore, a comprehensive overhaul of existing privacy frameworks is essential to effectively address AI-related challenges.

To regulate the rising challenges posed by AI to data protection in Nigeria, the NDPC as the primary regulatory authority needs to promote policies, strategies and practices that encourage fair and transparent handling of personal data, legality, accuracy, and privacy by design.

REPOSITIONING THE NIGERIA DATA PROTECTION COMMISSION IN THE ERA OF ARTIFICIAL INTELLIGENCE

Globally, DPAs are increasingly acting as regulators for AI technologies. For example, initiatives such as the European Data Protection Board's ChatGPT Taskforce, investigations and lawsuits in Italy, Poland, and Germany, and the CNIL's action plan for Artificial Intelligence in France, highlight how regulators respond to privacy concerns associated with AI.

Various DPAs including the United Kingdom's Information Commissioner's Office, Canada's Office of The Privacy Commissioner, and South Korea's Personal Information Protection Commission, have developed soft laws (guidelines, principles, and toolkits) to clarify how existing legal frameworks apply to these technologies.

It is crystal clear that in many parts of the world, Data Protection Authorities have repositioned themselves as de facto AI Regulators to meet up with the rapid technological advancements.

Although the NDPC has not yet fully dedicated any of its resources specifically for the regulation of AI, it is possible to infer an effort to regulate AI from various directives and policies issued by the Commission.

The General Application and Implementation Directive (GAID) was issued by the NDPC in March 2025, to take effect from September 2025. The GAID is meant to provide guidance, 'particularly in the space of disruptive technologies and shifting paradigms of engagements – involving the processing of personal information – among citizens, organisations, communities, states and countries around the world'.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

According to Article 43 of the GAID, data controllers planning to implement ETs, including artificial intelligence, must consider the provisions of the NDPA, the GAID (and other relevant regulatory frameworks) as well as public policy, to ensure the protection of data subjects' privacy. The GAID encourages data controllers deploying AI systems that process personal data to align their practices with global standards, such as the United Nations Resolution on Artificial Intelligence. Article 29 of the GAID mandates a DPIA in cases of profiling and automated decision-making. Data controllers and process are prohibited from using/deploying AI systems that pose undue risks to the enjoyment of human rights.

The Strategic Roadmap and Action Plan (SRAP) of the NDPC, was designed to guide the commission in discharging its mandate of ensuring a sustainable ecosystem for protecting data subjects' rights in Nigeria. Recognizing the significance of data in digital technologies and associated risks to human rights, including the right to privacy is central to this initiative. The Governance pillar of the SRAP seeks to cultivate a progressive legal, policy, administrative, and regulatory regime for data protection and privacy in Nigeria. In this Pillar, the commission recognizes AI Advancements and other large-scale data processing activities as strategic issues that must be tackled by developing and enforcing appropriate regulations to strengthen the ecosystem.

To translate theoretical concepts into practical applications, the NDPC has begun efforts to collaborate with private sector stakeholders in Nigeria. This initiative involves the establishment of regulatory sandboxes designed to facilitate the integration of AI within data protection frameworks. The primary objectives of these sandboxes are to promote responsible AI usage, ensure compliance with the NDPA, and enhance trust, fairness, accountability, and transparency in data management practices.

RECOMMENDATIONS

Organizational Accountability: While awareness and education of the public remain paramount, the weight of ensuring privacy in the deployment of AI tools must be shifted to organizations rather than placed on individuals.

- The AI landscape is complicated and constantly evolving. Erstwhile regulations on privacy have laid an emphasis on 'the right to informational self-determination', that is, individuals possessing access, authority, and control over their personal data and how it is used. This forms the basis of the right to be informed, the right to rectification, the right to data portability and the right to be forgotten. However, in terms of AI, it is practically impossible for individuals to exercise this sort of control, especially in terms of the billions of datasets used to train AI Systems. Rather, Regulators like the NDPC should push for higher levels of accountability on the part of deployers of AI Systems. Compulsory Data Privacy Impact Assessments and AI audits are some measures to ensure compliance with Privacy Laws and implement privacy by design. While the NDPC has made a significant initial move by mandating DPIAs in the GAID, it is essential to evaluate the effectiveness of these assessments. Follow-up reports and on-the-ground assessments are crucial to ensure that the DPIA framework is not merely a theoretical exercise, but rather an effective measure that prevents harmful privacy practices from continuing unchecked.

Interagency Cooperation: the job of regulating the privacy impacts of AI cannot be done by the NDPC alone. Privacy is a subject that cuts across different sectors of society – governmental, non-governmental, educational institutions, financial institutions, and other private business organizations. This is even more relevant as different organizations incorporate generative AI and automation in their day-to-day operations.

It is paramount for the NDPC to collaborate with other governmental agencies and private organizations like the FCCPC, Central Bank of Nigeria, Nigeria Police Force, National Human Rights Commission and Nigeria Labor Congress to raise awareness on AI integration and how it impacts the right to privacy and other fundamental human rights of Nigerians in different facets of society to ensure a safe and secure digital environment for all members of the populace.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

- Regulatory Sandboxes: Create regulatory sandboxes and strategic roadmaps that address each phase of the data life cycle to proactively manage specific challenges. Tailored solutions should be developed for issues related to data generation and collection, focusing on transparency. For concerns around outputs and inferences, emphasis should be on accountability, due process, and enforcement. Oversight should be prioritized for surveillance and high-risk AI systems.

- Education and Awareness: Regular workshops and seminars can serve as platforms for engaging discussions, allowing experts to share insights on the ethical implications of AI and data privacy. Additionally, leveraging social media campaigns can reach a broader audience, disseminating vital information quickly and effectively. Advocating for the integration of AI ethics and data privacy into educational curricula at all levels will ensure that future generations are equipped with the knowledge to navigate these complex issues.

CONCLUSION

As AI technologies proliferate, the NDPC's role as a regulatory authority becomes increasingly critical. To foster a robust AI ecosystem in Nigeria, the Commission must not only establish comprehensive regulatory frameworks that promote ethical data use but also actively monitor and enforce compliance with these regulations. By prioritizing accountability among organizations deploying AI systems, the NDPC can ensure that privacy rights are respected and upheld. This involves implementing mandatory Data Protection Impact Assessments (DPIAs) and encouraging interagency cooperation to address the multifaceted challenges posed by AI. Moreover, fostering public awareness about data privacy rights will empower citizens to navigate the complexities of an AI-driven landscape. Ultimately, the NDPC's proactive leadership will be essential in shaping a future where technological innovation aligns with the fundamental rights of individuals. By embracing its role as a guardian of data protection in this era, the NDPC can help build a digital environment that not only drives economic growth but also safeguards the privacy and dignity of all Nigerians.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

REPOSITIONING DATA PROTECTION AUTHORITIES IN THE ERA OF ARTIFICIAL INTELLIGENCE: NIGERIA AS A CASE STUDY

By
FAWAZ

1. INTRODUCTION

French President, Emmanuel Macron earlier this year, kicking off a 2-day AI summit in Paris, announced a €109 billion plan to boost artificial intelligence in France. Macron presented the French plan as a response to 'catch up' to President Donald Trump's January 21st's €500 billion 'stargate' initiative. Artificial Intelligence (AI) is no longer a concept of the future; it is already a 1 part of our present, actively being integrated and utilized across various sectors and aspects in our daily lives. These systems are transforming every walk of life, they are now being increasingly utilized to make critical predictions or decisions about individuals; this includes fields such as finance, national security, health care, criminal justice, and transportation. For instance, an AI model achieved 94% accuracy in detecting breast cancer in mammograms.2 Last year, Demis Hassabis and John M. Jumper were awarded the 2024 Nobel Prize in Chemistry for developing an AI algorithm that solved the 50-year protein structure prediction challenge. Likewise in finance, In August 2025, the world's first AI powered bank, Ryt Bank was 3 launched in Malaysia offering personalised banking experiences to customers through interactions based on individual preferences and habits like any other traditional bank would. 4

AI is here to stay, as global tech icon Bill Gates put it "It will change the way people work, learn, travel, get health care, and communicate with each other…Entire industries will reorient around it. Businesses will distinguish themselves by how well they use it.". A project undertaken by 5 PriceWaterhouseCoopers estimated that AI technologies could increase global GDP by $15.7 backbone of the global AI industry.

The emergence and popularity of generative AI have not 7 only cemented NVIDIA's position, a traditional graphics-chip designer, at the center of the artificial intelligence boom but have also reshaped our daily interactions, learning processes, policymaking, perspectives, social media, and even international relations further fueling a growing technological rivalry between the United States and China.8

The rapid pace of AI development, coupled with its transformative potential, has naturally led to concerns and uncertainty. Job displacement, bias, privacy and piracy are among the top ethical and social concerns associated with artificial intelligence, posing significant threats to its development in globally and of course in Nigeria. Companies around the world have expectedly 9 increasingly turned to job cuts amid weakening consumer sentiment and the growing adoption of AI-driven automation that is swiftly beginning to replace human roles. In September 2025, creators of Claude another popular AI Large Language Model (LLM), Anthropic agreed to pay $1.5 billion in a class-action settlement brought by authors and publishers who alleged the company used nearly 500,000 copyrighted books downloaded from pirate sites to train its large language models.10

While AI will present new possibilities and opportunities for economic development, it poses unprecedented challenges for governments worldwide especially in areas of regulating it. As expected, AI mentions in global legislative proceedings rose by 21.3% in 2024, reaching 1,889 mentions compared to 1,557 in 2023, and marking a ninefold increase since 2016.11

Countries are ramping up efforts to regulate AI and empower data protection authorities with powers and capabilities to address its challenges. This essay highlights the urgent need for While AI offers tremendous opportunities for improving lives worldwide, it is crucial to develop a regulatory framework that mitigates potential risks, harms and ensures that everyone, regardless of nationality or socioeconomic status, can benefit from this technology.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

To secure their leadership position in the AI realm, as expected the developed nations are actively developing and discussing specific laws aimed at monitoring, and regulating these AI systems while still fostering innovation and competitiveness.

While AI offers tremendous opportunities for improving lives worldwide, it is crucial to develop a regulatory framework that mitigates potential risks, harms and ensures that everyone, regardless of nationality or socioeconomic status, can benefit from this technology. To secure their leadership position in the AI realm, as expected the developed nations are actively developing and discussing specific laws aimed at monitoring, and regulating these AI systems while still fostering innovation and competitiveness.

In March 2024, the European Union (EU)'s comprehensive AI Act received parliamentary approval and came into effect on August 1, 2024 across all 27 EU Member States. It stands 12 out as the world's first standalone AI regulation. While many nations are still considering this and other approaches, others, like the United Kingdom (UK), Switzerland, and Japan, are adapting existing laws for AI. The United States (US), though lacking a unified AI law, is employing a case-by-case strategy and exploring various AI governance proposals. These efforts of these governments appear to align with the principles of the Bletchley Declaration, a global agreement signed by 28 countries and the EU at the AI Safety Summit.13

Nigeria, also one of the signatories to the Declaration, however lacks a formalized national AI specific regulation nor policy. The nation currently has sector-specific laws that, while not explicitly designed for AI, remain relevant in its context. These include the Cybercrimes (Prohibition, Prevention, etc.) Act, the Copyright Act of 2022, the Security and Exchange Commission (SEC) Rules on Robo-Advisory Services, and the Nigerian Communication Timely implementation and enforcement of AI regulations are crucial to mitigating potential risks for any country. The nation's reputation for slow implementation of critical initiatives raises questions about its ability to effectively address AI-related challenges.

However, The Nigerian government demonstrates its commitment to fostering AI research, innovation and regulation through initiatives like the National Information Technology Development Agency (NITDA), as it diligently works toward crafting a National Artificial Intelligence Policy (NAIP) and the National Centre for Artificial Intelligence and Robotics (NCAIR). In August 2024, the conjoined effort of the NITDA and the Federal Ministry of Communication, Innovation and Digital Economy (FMIDCE), through the NCAIR resulted in the publication of the draft of the inaugural National AI Strategy (NAIS) which "sets a path to achieve the vision to be a global leader in harnessing 14 the transformative power of AI through responsible, ethical, and inclusive innovation, fostering sustainable development through collaborative efforts".15

The NDPR faced criticism for its limited scope, lack of an independent enforcement authority, and its origin as a government agency rather than a product of parliamentary deliberation. These shortcomings, combined with its inability to keep pace with evolving international standards, led to the very enthusiastic reception of the NDPA, which was passed in June 2023.

The NDPA significantly addresses many of its predecessor's shortcomings. It establishes and transfigures the Nigeria Data Protection Bureau into the 'independent' NDPC, mandated to 16 foster data protection technologies, and promote international best practices. The NDPA also importantly extends its scope to cover data processing within Nigeria, regardless of the data volumes of Nigerian data subjects or data of significant value to the country. while not directly addressing AI-specific concepts, provides a strong foundation for proper AI regulation by outlining essential data protection principles. However, The NDPA introduces innovative provisions for Automated Decision making (ADM), ensuring individuals have control over data driven decisions without any human involvement. It prohibits data collection through ADM and 27 grants individuals the right to opt out of ADM-based decisions.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

3.0 PREPAREDNESS OF OUR DPA AND COMPARATIVE ANALYSIS WITH OTHER JURISDICTIONS

Despite these seemingly innovative provisions, the question remains whether they are sufficient to address the ever-growing demanding complexities of the AI era. AI's intricate algorithms and vast data requirements may still be unfamiliar to many Nigerian researchers, practitioners, and lawmakers. Costly infrastructure, dire short age of skilled personnel and risks in addition to earlier highlighted 'scanty' regulatory landscape are atop the list of challenges for us. The International Monetary Fund (IMF) has ranked Nigeria as significantly underprepared for the advent of AI, scoring the country just 0.34 on its AI Preparedness Index. 28

Simply put, better laws give our DPAs better authority. Nigeria's AI landscape is characterised by a lack of capable regulation, leaving society vulnerable to potential risks of misuse.

Comparatively, The EU AI Act came into force on August 1, 2024. This act employs a risk-based approach, classifying AI systems based on their impact risks. While minimal-risk systems are unregulated, unacceptable-risk systems are prohibited.

The act focuses on regulating 29 30 limited-risk systems and imposes stringent requirements on high-risk AI systems, which are 31 defined as those used in areas that could negatively impact safety or fundamental rights. The act primarily places obligations on providers, requiring them to establish risk management 32 systems, provide instructions for downstream deployers, design systems for human oversight, ensure data quality and security, and comply with technical documentation requirements.33 General-purpose AI (GPAI) systems are also subject to similar requirements, with an 34 additional mandate to respect the Copyright Directive. 35

Canada's proposed Artificial Intelligence and Data Act (AIDA) also adopts a risk-based approach. focusing on "high-impact" AI systems. These include systems affecting access to 36 services or employment, biometric systems, behavior-influencing systems, and critical health and safety systems.

The AIDA also uniquely addresses systemic bias in AI, requiring entities 37 to assess and mitigate bias risks. It proposes that businesses developing such systems must identify and address risks, document usage, and adjust measures accordingly. It also 38 excellently creates new criminal offences and penalties for reckless or malicious uses of AI including, unlawfully or deceitfully obtaining personal information for AI development, deploying AI systems known to be likely to cause serious harm or substantial property damage and using an AI system with intent to defraud the public and cause substantial economic loss.

The penalties for non-compliance include fines of up to $25 million or 5% of global revenue. Unfortunately, despite these brilliant provisions, the AIDA, first proposed in 2022 is still not in effect as it has been thoroughly criticized for its lack of public consultation, jurisdictional issues, vague definitions of some provisions and its DPAs lack of independent regulatory oversight.

Our current legal framework In Nigeria and regulatory powers and capabilities cannot adequately mitigate the risks posed by these "high-risk, high-impact" AI systems.

4.0 LOOKING AHEAD: CONCLUSION AND RECOMMENDATIONS FOR REPOSITIONING

Advancements in general-purpose AI are accelerating rapidly as organizations invest in more computing power, data, and efficient algorithms. The commitment to and prioritization of AI innovation and development by some countries including even developing ones on par with Nigeria, properly placing them in positions to shape the future of AI-driven application and regulation.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

Recommendations for repositioning Nigeria's data protection authorities in the AI era include.

1. To effectively regulate AI, Nigeria should consider enacting a comprehensive AI-specific law, similar to the EU and Canada's proposed AIDA. This would empower regulators with the necessary tools and expertise to address the complex challenges posed by high-risk AI systems.

balance between compliance and innovation. Excessive regulations can also hinder AI development and discourage developers, leading to potential economic and technological setbacks.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

THE STATE OF COMMUNICATION SURVEILLANCE LAW IN NIGERIA: FIT FOR PURPOSE OR NEED FOR REFORM?

BY
OBIORA VICTOR CHIBUZOR

1.0 INTRODUCTION

Communication surveillance is an essential tool used by governments around the world to combat crime and maintain national security. However, striking a balance between effective surveillance and protecting individuals' rights to privacy is a constant challenge. This paper aims to shed light on the state of communication surveillance law in Nigeria and evaluate whether it is fit for purpose or in need of reform. By examining existing legislation, analyzing recent cases, and exploring public opinion, this paper seeks to provide a comprehensive overview of the current state of communication surveillance in Nigeria.

2.0 LEGAL FRAMEWORK

The state of communication surveillance law in Nigeria is a complex and evolving one. The country has a number of laws that govern the interception and monitoring of communications, but these laws have been criticized for being outdated and not adequately addressing the challenges posed by new technologies. The primary law governing communication surveillance in Nigeria is the Nigerian Communications Act (NCA) 2003. The NCA empowers the Nigerian Communications Commission (NCC) to issue licenses to telecommunications operators and to regulate their activities. The NCA also contains provisions that allow the NCC to intercept and monitor communications in certain circumstances.

For example, the NCA allows the NCC to intercept communications if it has reasonable grounds to believe that the communications are being used for the purpose of committing or facilitating the commission of a crime. In addition to the NCA, there are a number of other laws that may be relevant to communication surveillance in Nigeria. These include the Cybercrime Act 2015, the Anti-Terrorism Act 2013, and the National Security and Intelligence Agency Act 2004. The Cybercrime Act 2015 prohibits a wide range of cybercrimes, including hacking, child pornography, and cyberstalking. The Act also gives law enforcement agencies the power to intercept and monitor communications in order to investigate cybercrimes.

The legal framework for communication surveillance in Nigeria is complex and fragmented. The laws that govern communication surveillance are often outdated and do not adequately address the challenges posed by new technologies.

3.0 FLAWS IN THE CURRENT SYSTEM

3.1 Lack of Judicial Oversight: One of the most significant issues with Nigeria's communication surveillance laws is the absence of adequate judicial oversight. This lack of checks and balances leaves room for abuse and unchecked infringement on individual privacy rights. In MTN Nigeria Communication Limited v Barr. Godfrey Nya Eneye, The Court held that the unauthorized disclosure of a mobile phone number is a violation of the right to privacy. In this case, the plaintiff sued his telecommunications service provider for disclosing his mobile phone number to a third party without his consent. The Court held that the disclosure of the plaintiff's mobile phone number was a violation of his right to privacy. The Court awarded the plaintiff damages for the violation of his privacy. This case is significant because it recognizes the right to privacy in the context of telecommunications. The Court's decision highlight the need for greater judicial oversight of communication surveillance.

3.2 Scope Creep and Mission Creep: The broad language used in the existing legislation allows for the expansion of the surveillance mandate beyond its original purpose. This phenomenon, known as scope creep, enables agencies to surveil citizens for reasons unrelated to cybercrime.

Mission creep refers to the expansion of surveillance powers beyond reasonable limits, ultimately eroding civil liberties. These tendencies undermine the trust citizens should have in their government and law enforcement agencies. In a 2020 survey by Paradigm Initiative, 70% of respondents expressed concern about the level of government surveillance in Nigeria.

3.3 Lack of Transparency and Accountability: The current state of communication surveillance law in Nigeria lacks transparency and accountability mechanisms. Citizens are often unaware of the extent to which their communications are being monitored. Additionally, law enforcement agencies are rarely held accountable for any violations of privacy rights. This lack of accountability only perpetuates a culture of surveillance and undermines the basic principles of democracy.

3.4 Chilling Effect on Free Speech: The oppressive nature of communication surveillance in Nigeria has had a chilling effect on free speech and expression. Citizens are often hesitant to voice dissenting opinions or engage in critical discussion on online platforms. This suppression of free speech stifles democratic discourse and prevents the growth of an informed and engaged citizenry. According to a 2023 report by Privacy International, Nigeria is one of the top 10 countries in the world with the most intrusive surveillance laws.

4.0 CASE STUDIES

In recent years, several high-profile cases have highlighted the need for evaluating the effectiveness and fairness of communication surveillance practices in Nigeria. One chilling tale involves Jerry Edoho, a journalist from the depths of Ibom Nation, Uyo, who found himself ensnared by the long arm of the law on that fateful January 2, 2017, accused of sowing discord on Facebook, where he dared to whisper the ominous prophecy of an airline disaster.

In the sinister symphony of suppression, Aku Obidinma, a broadcaster, met a similar fate, imprisoned on November 21, 2016, only to taste the bittersweet release on January 17, 2017, after enduring 60 days of desolation. His crime? Voicing his grievances on Facebook, a virtual graveyard for critics of the Imo State government.

The darkness deepened as Audu Maikori, a prominent businessman, was shackled by the chains of tweets he had weaved regarding the bloodshed stretching from southern Kaduna to the heart of northern Nigeria. Despite his retraction and admission of falsehood, justice remained elusive. Only a court's feeble attempt in October, like a flickering candle in a hurricane, ordered compensation for his wrongful imprisonment.

The somber procession continued with Austin Okai's arrest on April 9, 2017, in the heart of Abuja. His transgression? Expressing thoughts in the media deemed intolerable by the iron fist of the Kogi State government. Midat Joseph, head of the Bureau of Newspaper Management in Kaduna State, was the next victim, apprehended on April 19, 2017, for supposedly sowing the seeds of rebellion in a WhatsApp group, beckoning for protests against the slaughter of innocents. June 2 witnessed the physical embodiment of darkness as Charles Otu, a correspondent for The Guardian, became a target in Abakaliki. His only sin was his audacity to criticize the Ebonyi State government on Facebook, inviting the wrath of those who shroud the truth in shadows. On June 15, 2017, the tale of Danjuma unfolded, his voice stifled in Katsina for daring to question the legitimacy of a newly elected representative of the Nigerian House of Representatives.

Johnson Musa, too, felt the cold touch of suppression as State Security Service agents apprehended him. His transgression? A mere image of the governor's residence in Abuja State, shared on WhatsApp, accompanied by words deemed unholy by the authorities. The relentless storm continued its march as, on January 19, the hallowed halls of Premium Times, a bastion of journalism, were violated by the Nigerian police. In the wake of defamation claims, their publisher and legal correspondent found themselves ensnared, their sanctuary violated without warrant, further dimming the flickering beacon of truth.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

While these arrests may be seen as positive outcomes resulting from communication surveillance, there are concerns about potential abuses and violations of the suspects' rights during the investigation process. It is crucial to examine the legal framework governing such monitoring to ensure it aligns with internationally recognized human rights standards.

5.0 RECOMMENDATIONS FOR REFORM

Based on the overview of the current state of communication surveillance laws in Nigeria, the following recommendations are proposed for reform:

5.1 Clarification and Narrowing of Provisions: The Cybercrime Act should be reviewed to provide clearer definitions of what constitutes threats to national security and public safety. This will help prevent arbitrary interpretations and potential abuse.

5.2 Judicial Oversight: Introduction of a robust system of judicial oversight is vital to ensure that interception, monitoring, and seizure of communications are done lawfully, with proper adherence to due process and respect for privacy rights.

5.3 Transparency and Accountability: Government agencies responsible for communication surveillance should be required to publish annual reports detailing the nature and extent of surveillance conducted. This will enhance transparency and allow for public scrutiny and accountability.

5.4 Public Education and Awareness: The government should invest in public education campaigns to raise awareness about communication surveillance practices, their purpose, and the safeguards in place. This will help build trust and dispel misconceptions.

6.0 CONCLUSION

The state of communication surveillance law in Nigeria appears to be in need of reform. Although the Cybercrime Act was enacted to combat cybercrime and ensure national security, it lacks clarity and sufficient safeguards to protect individuals' privacy and freedom of expression. Recent cases and public opinion indicate growing concerns about the abuse of communication surveillance powers. By implementing the recommended reforms, Nigeria can strike a balance between effective surveillance and protecting citizens' rights, ensuring its communication surveillance laws are fit for purpose in the digital age.

THE STATE OF COMMUNICATION SURVEILLANCE LAW IN NIGERIA: FIT FOR PURPOSE OR NEED FOR REFORM?

BY

SIKAKU ONYINYECHI SANDRA

ABSTRACT

In recent times, states have recorded a surge in seeking access to communication metadata and content. This has the potential to intrude on and reveal the entire profile of an individual's life, including political and religious opinions, interests, associations, and medical history, and can enable the mapping of a person's interactions and location over time. While this may be largely due to security purposes, investigation of criminal activities, and protection against threats, It is imperative that the right to privacy is not sacrificed on the altar of the right to public health. This essay aims at appraising the state of communication surveillance law in Nigeria, examining its merits and shortcomings, and highlighting areas for possible reforms.

INTRODUCTION

Communication surveillance refers to the interception, monitoring, collection, analysis, preservation, use, and retention of or access to information that arises from or reflects a person's communication in the past, present, or future.

Nigeria's response towards maintaining internal security dates back to the colonial era, when the British mobilized all instruments of coercion in order to achieve total submission of the people. During the military rule, surveillance laws in Nigeria were targeted at monitoring the activities of political oppositions against coups. Nigeria's transition to democracy in 1999 conferred constitutional rights on citizens, which include the right to privacy and freedom. The digital and technological era, characterized by numerous security threats has introduced some modifications to surveillance laws and methods adopted by the government.

In other words, legislation such as the Cybercrime Prevention Act, 2015, the Nigeria Data Protection Regulation (NDPR), 2019, the National Security Agencies Act, the Nigerian Communications Act, 2023, the Nigerian Data Protection Regulation (NDPR), 2019, the Freedom of Information Act, 2011, and the most recent, the Data Protection Act, 2023, were enacted for the regulation of personal data and online activities.

In Nigeria, the primary regulation that recognizes the right to privacy as a fundamental human right is the 1999 constitution. The constitution guarantees the privacy of citizens, their family life, telephone conversations, and correspondence, and confers automatic protection on these rights.

However, despite the express recognition of the right to privacy as a fundamental human right, Nigeria has recorded numerous incidences of outright breaches, which reveals the inadequacy of its communication surveillance laws.

In 2017, for instance, the director of defense information made an announcement on the intervention of the military in monitoring activities on social media in order to stem out speeches and comments that are regarded as anti-military, security, or anti-government. Sequel to that, DSS effected the arrest of one Chisom Anaele in his home for alleged comments made on social media. In 2018, SARS agents arrested some Nigerian publishers (Daniel and Tim Elombah) for publishing an online article criticizing the IGP of the police. Most significantly, in 2020, the SARS operatives employed communication surveillance mechanisms to trace and detain some individuals who made tweets and comments strongly criticizing their actions during the ENDSARS protest.

In recent developments, there have been reports of the intention of the government to launch communication satellites with eavesdropping capabilities for conducting surveillance of mobile phones in the Federal Capital Territory of Abuja.

Amongst the legislation governing communication surveillance in Nigeria is the Terrorism Prevention Act, 2011. The Act authorizes "law enforcement agencies," with the approval of the attorney general and coordinator for national security, to apply to a judge for an order for the interception of communication for the purpose of combating terrorism and prosecuting offenders. The scope of the order allows law enforcement agencies to require communication service providers to intercept and retain specified communication for a stipulated period of time. The Act further grants law enforcement agencies the authority to enter upon any premises and install any device for the interception and retention of communication.

The Cybercrime (Prohibition and Prevention) Act, 2015, sets out a more robust regulation of communications surveillance in Nigeria. According to the Act, communication surveillance can be implored only in circumstances where there are reasonable grounds to suspect that the content of any electronic communication is required for the purposes of criminal investigation or proceedings. A judge can make an order authorizing service providers or law enforcement agencies to collect, record, intercept, or assist in collecting records associated with specific communications.

However, with the exception of the Nigerian constitution, neither the Terrorism (Prevention) Act, 2011 nor the Cybercrime (Prohibition and Prevention) Act, 2015, makes provision for communication surveillance to be carried out only when necessary and towards achieving a legitimate aim. The Acts only conferred wide discretionary powers on the judge in granting orders for surveillance, which could be exercised arbitrarily.

In terms of privacy concerns, according to global best practices on communication surveillance, the general rule requires that any person who is the subject of communication surveillance be notified of the reason for the surveillance. An exception to this would be in instances where there are deals that prevent the person from being given timely notification.

However, in Nigeria, the existing communication surveillance laws fail to make provision for the notification of individuals or groups who are subject to surveillance. The application for an order for carrying out surveillance is brought "ex parte," and consequently, target individuals or groups are kept in the dark until a criminal action is instituted against them in court and evidence gathered through surveillance tendered against them. The implication of this is that it undermines the individual's possibility of seeking redress for illegal surveillance.

On the issue of indiscriminate data retention, regulatory guidance and legislation in Nigeria, such as the Cybercrimes Prevention Act, 2015, make mandatory provisions requiring internet service providers to retain all information, traffic data, and subscriber information for a minimum period of twelve (12) months and two (2) years, respectively.

Service providers are further required to comply with requests from relevant authorities for the retention and release of information that reveals an individual's location, among other things. This mandatory provision on telecommunication companies poses significant implications for the right to privacy and freedom of expression as it defeats the ability of individuals to remain anonymous.

Significantly, in other jurisdictions, the state of surveillance laws closely aligns with international standards on human rights. The United Kingdom has an investigatory powers tribunal, which effectively discharges the responsibility of ensuring that communication surveillance mechanisms are transparent. Similarly, in Germany, there is a robust oversight, which requires that judicial warrants be issued for surveillance activities to be undertaken. This underscores the prevention of the abuse of surveillance powers by relevant authorities.

Flowing from the above, it is evident that communication surveillance laws in Nigeria fall short of global standards despite the recent enactment of the Data Protection Act, 2023. Therefore, the need to address the shortcomings of communication surveillance laws in Nigeria is imperative. In order to better protect the right to privacy, the following reforms should be considered:

Comprehensive legal framework: Laws that are specifically targeted at regulating surveillance operations should be developed. These laws must clearly affirm the right to data protection and privacy, prescribe procedures for lawful processing and interception of personal data, and provide for an independent and impartial authority to act as a watchdog on the effective implementation of the law. These laws must reflect modern methods of communication surveillance and uphold the protection of fundamental human rights. Moreso, reforms and amendments should be made to existing legal and regulatory frameworks to ensure that they comply with international human rights standards.

Judicial Oversight: The concept of independence of the judiciary must go beyond mere letters and be given life. The government must take proactive measures to strengthen independence and non-interference in the operations of the judiciary as it relates to reviewing surveillance requests and overall compliance with the provisions of the law.

Reform on security agencies: All departments of law enforcement agencies in Nigeria should be made to adhere strictly to the statutes creating them. This statute must clearly prescribe their powers, oversight mechanisms, and limitations of powers when involved in investigations requiring communication surveillance. Law enforcement agencies should be mandated to initiate disclosure of the type of surveillance technologies employed in the country and how they are regulated in order to achieve Nigeria's national and international obligations on data protection and privacy.

Conclusively, reform in communication surveillance laws in Nigeria cannot be actualized with sole reliance on the government and law enforcement agencies. There is a clarion call on various stakeholders, such as legal experts, human rights activists, journalists, and civil society organizations, to launch information literacy programs for the general public regarding the importance of privacy and the laid-down procedures for communication surveillance as provided by domestic and international legal frameworks.

This underscores the need for the government of Nigeria to ensure strict compliance with international human rights standards on issues of communication surveillance, as this would not only herald a significant milestone in data protection but also promote the image of the country on the global stage.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

THE STATE OF COMMUNICATION SURVEILLANCE LAW IN NIGERIA: FIT FOR PURPOSE OR NEED FOR REFORM?

BY
AWONUGA OLUWATOBILOBA PRAISE

ABSTRACT

In an era of rapid technological advancements, the need for effective communication surveillance laws is paramount. Nigeria, as an emerging economy, is no exception, requiring robust legislation to combat security threats while upholding citizens' rights. There is a need for an independent body or mechanism to ensure that communication surveillance activities comply with the law and adhere to international human rights standards. Such oversight would ensure transparency, accountability, and protection against abuse. Nigeria should consider strengthening its legal framework on communication surveillance, striking a balance between national security interests and the protection of individual rights. This essay critically examines the current state of communication surveillance law in Nigeria while highlighting its inadequacies and the dire need of reform to strike the right balance between national security and individual privacy, while aligning it with contemporary challenges and global standards.

INTRODUCTION

Nigeria, like many nations globally, faces a multitude of security challenges ranging from terrorism and cybercrime to money laundering and corruption. The government, in response, has implemented various communication surveillance practices to protect national security. The state of communication surveillance law in Nigeria has been a subject of concern for both legal scholars and human rights activists. Nigeria, like many other countries, has implemented various laws and policies to regulate the interception and monitoring of communication for national security purposes. However, there have been criticisms about the lack of adequate safeguards and oversight mechanisms to prevent abuse and protect the fundamental rights of individuals.

The key legislation governing such activities in Nigeria includes the Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 and the National Security Agencies Act of 1986. The state of communication surveillance law in Nigeria has been a subject of concern for both legal scholars and human rights activists. Nigeria, like many other countries, has implemented various laws and policies to regulate the interception and monitoring of communication for national security purposes.

However, there have been criticisms about the lack of adequate safeguards and oversight mechanisms to prevent abuse and protect the fundamental rights of individuals Communication surveillance is a crucial aspect of modern governance and national security. It involves the monitoring, interception, and analysis of electronic communications to protect citizens and safeguard national interests. However, striking a balance between surveillance and maintaining individual privacy and civil liberties is a complex task for any nation.

CURRENT LAWS ON COMMUNICATION SURVEILLANCE IN NIGERIA: THE FIT FOR PURPOSE ASSESSMENT

While the existing surveillance laws in Nigeria aim to safeguard national security, their effectiveness and efficiency fall short in many respects. To begin with, the legislation lacks clarity regarding the definition and scope of surveillance practices, causing uncertainty among citizens about their rights and the government's lawful actions. This ambiguity hinders the accountability and transparency necessary for an effective legal framework. Furthermore, the technological landscape evolves rapidly, rendering the current legislation outdated and incapable of addressing modern communication methods.

The laws primarily focus on telecommunications, ignoring emerging platforms such as social media, encrypted messaging services, and Voice over Internet Protocol (VoIP) communication, which are commonly used by criminals, making the surveillance laws insufficient in combating contemporary security.

While ensuring national security is crucial, it should not come at the expense of violating citizens' fundamental rights, including the right to privacy. The current legal framework in Nigeria allows for communication surveillance under the provisions of the 2015 Cybercrimes (Prohibition, Prevention, etc.) Act and the Economic and Financial Crimes Commission Act. These laws grant powers to various government agencies, such as the Nigerian Police Force, State Security Services, and National Intelligence Agency, to conduct surveillance operations for criminal investigations and national security purposes.

While the existing laws are aimed at addressing the growing challenges of cybercrimes and terrorism, they fall short in safeguarding individual citizens' privacy rights and upholding principles of transparency and accountability. While this Act aims to combat cybercrime and protect critical national information infrastructure, there are concerns about its broad provisions that could potentially infringe on the right to privacy and free expression. The laws lack clarity on the scope, limitations, and oversight mechanisms for surveillance operations, often leading to potential abuse of power and misuse of surveillance technologies. Inadequate safeguards and accountability mechanisms pose a significant threat to citizens' fundamental rights and undermine the trust between the government and its people.

The Act grants extensive powers to law enforcement agencies to intercept and monitor communication, without clearly defining the valid grounds and limited scope for such surveillance. This lack of specificity raises questions about the proportionality and necessity of these surveillance measures, as well as the potential for abuse.

RECCOMENDATIONS: AN AMELIORATION OF COMMUNICATION SURVEILLANCE

The need for reform is as important as humans needing oxygen to breathe. It is safe to say that it strengthens privacy protections. Nigeria should enact comprehensive legislation that explicitly recognizes citizens' right to privacy in the digital age.

The law should incorporate proportionality and necessity principles that restrict communication surveillance to situations where it is essential and where less intrusive means are not feasible. The reform must provide robust oversight mechanisms and strong safeguards against abuse and unlawful access to personal data. Currently, communication surveillance in Nigeria can be authorized by executive agencies without sufficient judicial oversight. Reforms should require independent judicial authorization based on reasonable suspicion and the necessity for interception, in line with international best practices. This will ensure a balanced approach where privacy rights are protected, and surveillance operations are subject to scrutiny and accountability.

Also, the reform must introduce transparency requirements, mandating regular publication of detailed surveillance statistics to accurately assess the scale and impact of surveillance practices. This will enable public debate and scrutiny, ensuring that surveillance actions are properly justified and aligned with democratic values. The existing laws do not adequately reflect advancements in digital technologies and the changing nature of communication. Reforms should address emerging issues related to encrypted communication, cloud storage, social media platforms, and other technological advancements.

This will help Nigeria to respond effectively to evolving threats while respecting privacy rights and digital freedoms. Surveillance reform in Nigeria should align with global standards and best practices to foster cooperation with international partners. Building alliances and participating in international forums will enhance Nigeria's knowledge exchange and capacity development in the field of communication surveillance, enabling the country to benefit from shared experiences and advancements made elsewhere. To address the inadequacies of communication surveillance laws in Nigeria, comprehensive reform is necessary.

Firstly, the legislation must incorporate clear definitions of surveillance practices and include provisions that accommodate emerging technologies and platforms, enabling law enforcement to effectively combat contemporary security threats.

Secondly, robust oversight mechanisms need to be established to ensure accountability and transparency. Independent bodies, such as a dedicated surveillance court or a surveillance regulator, should evaluate surveillance requests, monitor the activities of security agencies, and provide citizens with avenues for redress in case of abuses.

Furthermore, the reform should prioritize the protection of individual privacy rights. The legislation must include specific guidelines on data retention periods, purpose limitations, and the legality of warrantless surveillance. Safeguards such as notification requirements for targeted individuals and mandatory periodic audits of surveillance activities should also be put in place to uphold citizens' rights and prevent abuse of power.

CONCLUSION

In conclusion, the current state of communication surveillance law in Nigeria is inadequate, and urgent reform is needed to ensure a balance between national security imperatives and the protection of individual rights. By clearly defining the circumstances under which surveillance is permissible, implementing strong safeguards and oversight mechanisms, Nigeria can safeguard its citizens' rights while effectively combating the menace of cybercrime. Clarity, efficiency, and the inclusion of modern technologies in legislation, accompanied by robust oversight and safeguards, are essential to strike the appropriate balance. By enacting comprehensive reform, Nigeria can establish a communication surveillance framework that is fit for purpose, ensuring the safety of its citizens while respecting their privacy rights.

ASSESSING NIGERIA'S DATA PROTECTION READINESS IN THE AGE OF LARGE LANGUAGE MODELS (LLMS)

BY

IMOTER KELVIN KPENGWA

INTRODUCTION

The world has witnessed a rapid transformation in the digital landscape in recent years, marked by the emergence of cutting-edge technologies like Artificial Intelligence (AI). One of the most popular applications of this technology is Large Language Models (LLMs), a subset of Natural Language Processing (NLP). LLMs, such as OpenAI's GPT-3 and Google Bard, have revolutionized how we interact with data and information. They have become lifesavers for professionals in different fields, from medicine to research and art. The excellence of this technology begs the question: How can LLMs give such intelligent and human-like responses to queries? The simple answer is data. These systems are fed with tons of data to help them generate intelligent and human-like responses to user queries. In fact, the larger the data LLM is fed, the more potent it becomes. There is no doubt that where such a large volume of data is involved, the issue of data protection will arise.

This article will look at LLMs, how they work, and the data concerns raised by their use. Then, it will examine the data protection framework in Nigeria *vis-à-vis* other jurisdictions to assess her readiness to adapt to this global phenomenon.

Understanding LLMs

LLMs are foundation models that use AI, deep learning, and massive data sets, including websites, articles, and books, to generate text, translate between languages, and write many types of content. LLMs need to meet the user where he is to be considered adequate. They must understand language, its many contexts, nuances, and rare phenomena. LLMs must also be able to perform tasks beyond the scope of their training.

This is why all LLM training mechanisms involve exposure to massive datasets. While the definition of "large" has been increasing exponentially, these models are typically trained on datasets large enough to include nearly everything written on the internet over a significant time.

For example, in June 2020, OpenAI released GPT-3, a 175 billion-parameter model allegedly trained on 570GB of data scraped from the internet that generated text and code with short written prompts. In 2021, NVIDIA and Microsoft developed Megatron-Turing Natural Language Generation 530B, one of the world's most extensive reading comprehension and natural language inference models, with 530 billion parameters.

LLMs process the datasets through unsupervised learning, meaning they process the data without specific instructions. During this process, the LLM's AI algorithm can learn the meaning of words, the relationships between words, and how to distinguish words based on context. The enormous datasets used in training LLMs are what makes them revolutionary. Their uses extend far beyond the realm of language to the world of science. They can be used to write computer codes and even to develop vaccines. The application of LLM technology is limitless, and we are only now scratching the surface.

LLMs and Data Privacy

As already stated, LLMs raise many concerns regarding data protection. The first data privacy concern LLMs raise is whether the models' developers fall into the traditional data controller or data processor categories. A data controller determines the purposes for which and the means by which personal data is processed, while a data processor processes personal data on behalf of a data controller. Going by these definitions, LLM developers are data controllers in relation to the data they scavenge but are data processors where other entities use them to process their data.

LLMs also raise concerns regarding what kind of data is being collected and used to train LLMs and how long the data is stored. To answer the first question, LLMs are said to be trained with publicly available data, some of which may be private data. This is somewhat vague and implies that private data that became public data due to data breaches would be used to train these models. Social networking sites like Facebook, Reddit, Quora, YouTube, and Medium have been cited for training LLMs.

The current legal framework in Nigeria allows for communication surveillance under the provisions of the 2015 Cybercrimes (Prohibition, Prevention, etc.) Act and the Economic and Financial Crimes Commission Act. These laws grant powers to various government agencies, such as the Nigerian Police Force, State Security Services, and National Intelligence Agency, to conduct surveillance operations for criminal investigations and national security purposes. While the existing laws are aimed at addressing the growing challenges of cybercrimes and terrorism, they fall short in safeguarding individual citizens' privacy rights and upholding principles of transparency and accountability.

While this Act aims to combat cybercrime and protect critical national information infrastructure, there are concerns about its broad provisions that could potentially infringe on the right to privacy and free expression. The laws lack clarity on the scope, limitations, and oversight mechanisms for surveillance operations, often leading to potential abuse of power and misuse of surveillance technologies. Inadequate safeguards and accountability mechanisms pose a significant threat to citizens' fundamental rights and undermine the trust between the government and its people.

The Act grants extensive powers to law enforcement agencies to intercept and monitor communication, without clearly defining the valid grounds and limited scope for such surveillance. This lack of specificity raises questions about the proportionality and necessity of these surveillance measures, as well as the potential for abuse.

RECOMENDATIONS: AN AMELIORATION OF COMMUNICATION SURVEILLANCE

The need for reform is as important as humans needing oxygen to breathe. It is safe to say that it strengthens privacy protections. Nigeria should enact comprehensive legislation that explicitly recognizes citizens' right to privacy in the digital age. The law should incorporate proportionality and necessity principles that restrict communication surveillance to situations where it is essential and where less intrusive means are not feasible.

The reform must provide robust oversight mechanisms and strong safeguards against abuse and unlawful access to personal data. Currently, communication surveillance in Nigeria can be authorized by executive agencies without sufficient judicial oversight. Reforms should require independent judicial authorization based on reasonable suspicion and the necessity for interception, in line with international best practices. This will ensure a balanced approach where privacy rights are protected, and surveillance operations are subject to scrutiny and accountability.

However, the source of most of the data used in training these LLMs remains unknown. In its 2022 report, Language Model for Dialogue Applications (LaMDA), used to train Google Bard, vaguely alluded to 50% of its scraped data as ‘dialogs data from public forums’ without stating which forums it sourced data from. The lack of transparency regarding the source of the data used in training LLMs is a violation of data privacy in some jurisdictions.

For example, under Article 14 of the General Data Protection Regulation (GDPR), data subjects whose data is openly sourced have the right to know what data is being collected and why. In line with Article 14 of the GDPR, the Polish Data Protection Authority (UODO) imposed a fine of about 220,000 Euros on Bisnode, a data aggregation company headquartered in Sweden, for failing to inform data subjects about how it processed their personal data.

Given that developers of LLMs are not forthcoming with the specific sources of the data used to train their models, it is nearly impossible for data subjects to know if their personal data has been used to train the models. Even though the terms of use of Facebook, LinkedIn, and Twitter prohibit web scraping, it remains unknown whether or not they are used to train LLMs regardless, and if yes, the extent of personal data used. Indeed, the whole point of LLMs is to give intelligent human-like responses, and people use sites like the above to express the different contexts and connotations of language, making them appealing to LLM training.

Apart from data sourced from the internet, developers also use end-users' personal data, like profile information and conversations, to train their LLMs. OpenAI, developers of the popular GPT-3 model, admit using end-user data and their interactions with the platform to improve its performance. The amount and type of data used remain vague, as is the duration it is kept. It is important to note that the end-user can change their settings to prevent their data from being used to improve the system. However, the default setting gives OpenAI the right to use the personal data of its model's end-users to feed it. While it can be argued that OpenAI fulfills the GDPR's duty to inform data subjects of the use of their personal data here, there is no doubt that the transparency and duration requirements remain unmet.

Additionally, recent research showed that while LLMs are helpful for taking notes during eye surgery, they usually mix surgery notes with patients' medical history and symptoms, which is sensitive personal data protected under Article 9 of the GDPR.

In view of the above, there is reasonable cause to believe that LLMs could give rise to profiling because they analyze user data to give personalized responses. This was best exemplified in the Cambridge Analytica scandal, where data from Facebook was used to create psychological voter profiles for the 2016 United States election. With LLM technology, scandals like this will happen on much larger scales with little effort.

Finally, LLMs host tons of data, making them susceptible to cyberattacks and subject to the exposure of sensitive information. OpenAI's ChatGPT was recently the subject of the latter when it announced that ChatGPT's chart source code, Redis, used to store user interactions per session, had a bug that caused specific data leakage. This led to users having access to the chat conversations of other users and the exposure of payment-related information of some premium users.

Accessing Nigeria's Data Protection Readiness in the Age of LLMs.

The principal legislation regulating data protection in Nigeria is the Nigeria Data Protection Act of 2023 (NDPA). The NDPA established the Nigeria Data Protection Commission (NDPC) as the primary data protection authority in Nigeria. It also retained the Nigeria Data Protection Regulation 2019 (as amended) (NDPR) developed by the National Information Technology Development Agency (NITDA) pursuant to the NITDA Act 2007.

Thus, the NDPA and the NDPR are to operate conjunctively, although the former shall prevail where there is conflict.The NDPA, like the GDPR, gives data subjects the right to be informed about the use and retention period of the personal data collected. It also provides that the data subject must have given and not withdrawn consent for the data to be used.

According to the law, consent must be affirmative and not based on pre-selected confirmation and may be written, oral, or electronic. However, the legislation seems archaic as it does not consider the peculiarity of LLMs. As stated earlier, LLMs are data controllers and data processors; as such, it can be argued that the above requirements do not specifically apply to them.

Other than the above, the NDPA and NDPR are silent on LLMs and how they work. It remains uncharted territory as far as Nigeria's data protection laws are concerned. This is the major loophole in data protection in Nigeria today. Even though the above sections can be generalized to tackle data privacy issues arising from LLMs, such decisions would be innately flawed as the legislation did not anticipate their existence.

RECOMMENDATIONS

The trend of Nigerian legislation tailing contemporary issues appears to be the case in LLMs and data protection. Our principal law, the NDPA, appears unprepared to tackle the peculiar data privacy concerns raised by LLMs despite being passed into law recently. To keep up with the global trend, there is a need for Nigeria to create new legislation to tackle the growing AI phenomenon, including LLMs. This appears to be the trend worldwide with the passing of the European Union AI Act on 16 June 2023. The legislation would address the data privacy concerns discussed above and give a more robust regulatory framework for the growing AI industry.

For watertight protection of the right to data privacy of Nigerians, the legislation must first put the interests of data subjects above the interests of LLMs. Additionally, the law should:

Create an agency to oversee AI and LLM administration by issuing licenses, making periodic regulations, and other ancillary functions to tackle developing issues in the AI industry in Nigeria.

Mandate developers to acquire renewable licenses before their LLMs are allowed to run in Nigeria to ensure they adhere to regulatory standards.

Ban unrestricted web scraping in Nigeria and mandate developers to publish a comprehensive list of the type and sources of the data used in training their LLMs, including the duration such data is used.

Mandate developers to be transparent about the application of the data obtained at the point of training or from end-users and the scope of its use.
Create penalties for breach.

With the above provisions, the law could address the live issue of data protection in light of LLM technology.

CONCLUSION

LLMs have rightfully taken the world by storm. They make work easier for professionals in many fields and have revolutionized vaccine technology. However, LLMs pose a severe data privacy threat with their existence and functionality. Some of these threats and the ways to address them have been discussed above. In curtailing the harm that these models can cause, it is pertinent that lawmakers put the rights of data subjects above the profitability of LLMs. Only then can the data privacy rights of individuals be preserved in today's data-insatiable economy.

ASSESSING NIGERIA'S DATA PROTECTION READINESS IN THE AGE OF LARGE LANGUAGE MODELS (LLMS)

BY
TEMILOLA ADETONA

INTRODUCTION

Data, they say, is the new oil. Although, that description is admittedly a bit of a hyperbole, in today's increasingly digital world, very few would contest the perceived and actual importance of data. Laudably, many jurisdictions have taken data protection seriously and, therefore, introduced significant policies and laws aimed at regulating data use and protection.

However, technological development evolves faster than we can prepare for it, with the consequent implication being that policy often trails advancement. It is perhaps against this background that Punit Bhatia has remarked that "Data protection is not a goal, it is a journey". This author reckons this comment to be accurate, and the quest of nations to ensure that the adequacy of their data protection regimes in the era of Large Language Models (LLMs) adequately illustrates how data protection is indeed a journey, an oft unfinished journey. Accordingly, this piece seeks to circumspectly examine whether Nigeria's data protection regime is indeed fit for purpose in the age of LLMs.

CONCEPTUAL BACKGROUND

If the foundation be destroyed, what shall this author do? It is, therefore, pertinent at this stage to interrogate, albeit briefly, the key concept that informs the central theme of this piece, viz: LLMs.

An LLM can be described as an artificial intelligence (AI) model trained on great amounts of data subtexts to comprehend and generate human-like language. To achieve this aim, LLMs utilise deep learning techniques, particularly deep neural networks, to process and generate text.

Generally, they are characterised as 'large' since they are built with a vast number of parameters and demand substantial computational power to train and run successfully. Put simply, an LLM is a variant of machine learning that is trained on a large dataset with a view to interpreting and generating human like text.

LLMs and Nigeria's Data Protection Regime: Ready or Not?

It is crucial at this juncture to consider whether Nigeria's current data protection framework is equipped to successfully protect the data of Nigerians in the era of machine learning. Thus, this segment provides: an overview of Nigeria's data protection regime; an assessment of its fitness for purpose; an identification of existent gaps; and recommendations to plug said gaps.

Overview of Nigeria's Data Protection Regime

"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds." – John Perry Barlow.

Whilst Barlow's sentiments above may resonate with many, the creation of a framework for data protection is a function that is best left to the remit of the government. Accordingly, the Nigerian government has attempted to provide a framework over the years, the evolution of which has ultimately culminated in the Data Protection Act (DPA) 2023 (the Act).

Whilst it is impossible to provide a comprehensive overview of the Act in this brief piece, it should be generally noted that the Act applies to the processing of personal data, notwithstanding whether such processing is undertaken by automated means or otherwise. The ambit of the Act is triggered where: (a) the residence or place of operation of the data controller is in Nigeria; (b) the processing of the personal data is undertaken in Nigeria; or (c) although the data controller or processor is domiciled, resident or operating outside Nigeria it undertakes the processing of personal data belonging to a data subject in Nigeria.

The culmination of the foregoing is that where the aforementioned requirements and thresholds are met, the processing of personal data via LLMs falls within the ambit of the Act. However, the question lingers as to whether the regime of the Act is adequately equipped to cater for nuances presented by the advent of LLMs.

Is Nigeria's Data Protection Regime Fit for Purpose?

On the face of it, it would appear that the general principles contained in the Act apply to and govern the processing of data via LLMs. The Act demands that those who are categorised as data controllers or processors must: (a) engage in a 'fair, lawful, and transparent' processing of data; (b) ensure that data is only collected for 'specific, explicit and legitimate' purposes (purpose limitation); (c) in light of the purpose, only collect data that is 'relevant, necessary and adequate' (data minimisation); (d) not hold the data longer than necessary (storage limitation); and (e) ensure the confidentiality, integrity, and security of data collected. Furthermore, the Act (x) imposes a duty of care on the data controllers and processors when processing personal data; (y) requires them to demonstrate accountability; and (z) explicitly sets out the six lawful bases for processing personal data.

Although AI and LLMs are not specifically mentioned in the Act, entities who operate LLMs are bound to comply with these internationally accepted principles in the operation of the models, thus creating a base framework for the regulation of data processing by LLMs in Nigeria. However, the nuanced nature of LLMs creates a tension between these traditional principles and the evolving data processing activities of LLMs which warrants specific consideration.

Nuances, Gaps, and Limitations

As stated earlier, the operation of LLMs is predicated on training the language model on large volumes of data. The sheer volume of data required to be fed into the LLMs is the principal precursor of privacy and data protection concerns especially as regards the nature of the data supplied to the LLM, data security, and the length of time for storing such data.

This operational model of LLMs discloses certain nuances and therefore reveals some gaps in the present data protection framework which must be plugged. Some of these include:

Application of the principles: Some of the most fundamental principles of direct data collection are that: (i) the data is collected for a specific purpose; (ii) the data subject is notified of the lawful basis for processing; and (iii) the data subject is informed of the recipients or categories of recipients of the processed data. One wonders if LLMs can duly satisfy these principles given that there will likely be significant downstream uses which may not remain within the scope of the stated purpose and the range of potential recipients may be too large to conceive or even specify. How effective then is the consent of the data subject where the use to which the processed data is put exceeds the originally agreed scope?

Use of publicly available data: The data upon which the LLMs are trained are often obtained from a wide variety of sources including the internet. This may, therefore, include information made available by individuals themselves on websites, blogs, social media, etc, although without any intention that such information is to be used by LLMs for whatever purpose. Where personal data is collected indirectly the data controller is required to inform the data subject of the lawful basis for processing, the proposed recipients of the processed data, retention period, and the identity of and means of communication with the data controller. This information may be provided in a clear and accessible privacy policy.

Further, the Act also provides an exception in that the data subject may not be informed where providing the information would involve disproportionate effort or expenses for the data controller. It is unclear how the privacy policy rule helps LLMs with regards to data fetched indirectly from sources such as social media pages.

For instance, if the LLM is trained on data fetched from social media, it is unclear how the LLMs general privacy policy may be communicated to all individuals concerned. On the other hand, there remains the possibility that the LLMs may opt to rely on the disproportionate effort or expenses exception.

Data security: There are also concerns that the large volumes of personal data collected, held and processed by LLMs are subject to a real risk of data loss or theft by hackers or other sinister persons who may then extract sensitive personal identifiable information. An indication of this risk occurred recently with ChatGPT when it was reported that a bug was found in the model's source code which resulted in some data leakage including conversation history and even payment related data. The Act prescribes that where a breach occurs the data controller/processor is to provide notification to the Nigerian Data Protection Commission and the data subject. One wonders if LLMs that process vast volumes of data are equipped to meet this obligation.

Right to be forgotten: The Act confers a number of rights on Nigerians one of which includes the right to request a data controller to erase their data from the database of the LLM. However, we question how this right can be enforced and how LLMs that have been 'trained' on the data in question can be made to 'forget' the data.

International data transfer: In light of the ubiquitous nature of LLMs, there is a great likelihood of data transfer across border. Whilst the Act does make provision, in principle, for regulating such transfers, procedural constraints exist such as the ability of the regulator to confirm if any data has been transferred across border, where such data has been transferred to, and if the recipient countries meet the adequacy of protection requirements.

RECOMMENDATIONS

It warrants emphasis that this piece does not in any way pretend to possess solutions to all of the gaps presented by the nuanced interaction of LLMs with the Nigerian data protection regime and the resolution of some of these issues can only be arrived at upon detailed technical consultation amongst regulators and stakeholders in the industry. Notwithstanding, in the immediate, this author presents the following propositions:

Regulators may need to consider and clarify the ways in which operators of LLMs may practically attain satisfactory compliance with existing principles under the Act.

Given that the Act draws inspiration largely from the GDPR, Nigeria can take a note from the EU's attempt to introduce a specialised AI Act that regulates the use and operations of machine learning tools such as LLMs. A law or policy in this regard, can attempt, amongst other things, to specifically address the management processes for the unique risks presented by AI powered models.

Rules need to be put in place to properly regulate the collection of publicly available data for the use of LLMs. At present, the principles do not envisage data collection at the volume of the LLMs and the exception that exists creates a situation where LLMs can consistently bypass their obligations to notify data subjects by simply claiming the disproportionate effort or expenses exception.

Regulators may also consider the imposition of: (a) bespoke obligations to implement more robust data storage and security measures; and (b) more stringent and specific pseudonymisation obligations on the entities that control LLMs to ensure that when data is collected at such mass volumes personal identifiers are removed which reduces risk to data subjects in the event of a data breach.

CONCLUSION

This succinct piece has sought to address the central question of the readiness and fitness for purpose of the Nigerian data protection framework in light of the growing presence of LLMs. In so doing, this author has concluded that the Nigerian regime, spearheaded by the Act, does contain traditional data protection principles that apply to LLMs and form an acceptable basic framework for regulation.

However, it has also been observed that there are nuances and consequent gaps which must be addressed in order to cater to the sui generis nature of LLMs. It is hoped that with subsequent stakeholder interaction the Nigerian data protection community can arrive at well considered and enduring solutions to risks posed by LLMs. A further hope exists that this is done in reasonable time as the deployment and use of LLMs grows by the day whether or not policy responds quickly. This situation inspires the author to recall the popular hide and seek 'call sign', ready or not, here I (LLM) come.

ASSESSING NIGERIA'S DATA PROTECTION READINESS IN THE AGE OF LARGE LANGUAGE MODELS (LLMS)

BY

BIBITAY EMMANUEL OJO

INTRODUCTION

In recent years, the proliferation of Large Language Models (LLMs) has revolutionised the field of artificial intelligence, enabling machines to generate human-like text at an unprecedented scale. While this technological advancement holds great promise for various sectors, it raises critical data privacy and protection concerns. Nigeria's landscape is not exempted from this astronomical eruption of generative AI and Machine Learning. However, the question is, how prepared is Nigeria to protect the data subject and the ethical use of the LLMs? This essay aims to assess Nigeria's preparedness in this evolving technological development and explore current initiatives, challenges, and potential strategies required to safeguard sensitive information in the age of LLMs.

Contextualizing Nigeria's Digital Transformation

The Information and Communications Technology (ICT) sector drives the rapid digitisation of various sectors in Nigeria. This sector plays a vital role in the country's economic recovery, contributing 9.88% to the GDP in Q4 of 2021. Nigeria's ICT market is the largest in Africa. It is projected to experience significant growth in the next few years as the wave of technological advancement is sweeping across every sector. The government recognises the importance of this sector and encourages partnerships with foreign investors. Furthermore, the Federal Ministry of Communications and Digital Economy has launched a national policy to diversify the economy. The ICT sector contributes about 17.47% to the country's GDP. It is reshaping the economic landscape of Nigeria and Africa through digital transformation.

Against this backdrop, there is much reliance on data-driven technologies for economic growth and development in reshaping the economic landscape of Nigeria and Africa. Nigeria's Information and Communications Technology (ICT) sector drives this transformation. Data and information have become significant drivers of economic growth and sustainable development in the 21st century.

The lack of data management systems in many African countries, including Nigeria, has led to negative consequences such as economic hardship and poverty. Recognising the importance of data-driven policies, the Nigerian government is partnering with operators to protect consumer data and ensure a secure economic environment. The National Information Technology Development Agency (NITDA) is actively working to promote a data-driven economy and national database development in Nigeria.

Overview of existing data protection laws on LLM in Nigeria

As of today, there is no specific law or regulation in Nigeria that addresses large language models or artificial intelligence systems. However, Nigeria enacted the Nigeria Data Protection Act in June 2023, which aims to protect personal data and promote the use of data-driven technologies for economic growth and development. While this Act focuses on data protection and privacy, it does not explicitly address the regulation of LLMs or AI systems. It is important to note that regulating AI and large language models is a global concern, and various countries are proposing laws to address their risks and impacts.

While LLMs and AI pose risks related to privacy and security, regulations such as the EU AI Act, UK AI Act, and Canada Artificial Intelligence and Data Act (AIDA) suggest the proactiveness of other jurisdictions to regulate this space. These laws aim to regulate the development and use of AI systems, including provisions for privacy and cybersecurity.

Conversely, the NDPA and NDPR have not given attention to the potential effects of generative AI on the rights and freedom of data subjects. Key clauses regarding algorithmic accountability and fairness are absent from Nigeria's data privacy framework. Without such provisions in the data protection regulations and laws, holding algorithms accountable will remain uncontrollable.

Likewise, there is no stipulated obligation to request a significant data controller to perform an Algorithm Impact Assessment in cases where training LLMs can pose a risk of data privacy breach. Similarly, a requirement for assessing algorithm designs could have averted numerous privacy breaches in LLMs. Unfortunately, this provision was also overlooked in the pertinent legal frameworks.

CHALLENGES POSED BY LARGE LANGUAGE MODELS

LLMs can affect personal data negatively in Nigeria. These models, such as ChatGPT and Google's Bard, can process and analyse massive amounts of personal data. The risks associated with LLMs include data privacy concerns, model bias and discrimination, security vulnerabilities, and data misuse.

If not properly regulated and managed, LLMs can lead to unauthorised access and misuse of personal data, compromising the privacy of individuals. Data subjects may also risk using their personal information in a biased or discriminatory manner, as large language models can inadvertently amplify existing biases present in the data they are trained on.

More so, the lack of transparency and accountability in LLMs can make it difficult for data subjects to understand how their data is being processed and used, compromising their rights to privacy and control over their data. While Nigeria does not have specific laws or regulations addressing LLMs, the Nigeria Data Protection Act 2023 provides guidelines and regulations for collecting, processing, storing, and sharing personal data, aiming to protect individuals' rights regarding their data.

Obtaining consent and transparency in data collection and processing is another main challenge, especially when training LLM. To ensure consent and transparency in data collection and usage of LLMs in Nigeria, a data controller/processor should adhere to the Nigeria Data Protection Act and its principles. The Act requires that consent be freely given, specific, informed, and unambiguous, similar to the consent requirements under the Nigeria Data Protection Regulation (NDPR). A data controller/processor must inform individuals about the purpose and scope of data collection and the intended use of LLMs in processing their data. Data subjects must obtain explicit consent before collecting and using their personal data.

However, the procedure for obtaining consent can be vague as users may only sometimes be fully aware of how their data is used. For instance, most users do not know that their interactions with ChatGPT are being stored and analysed. What about the data collected to train the LLM?

The potential for LLMs to amplify existing biases in data is a daunting risk to data protection in the age of AI. Like many machine learning systems, LLMs learn from vast amounts of historical data, which often contain inherent societal prejudices and biases. These biases can be perpetuated and even magnified when LLMs generate text or make decisions. For instance, if the training data contains biased language or stereotypes, LLMs may inadvertently produce content reinforcing these biases. This poses a significant threat to data protection, as individuals may face discriminatory outcomes in automated decision-making processes, and their privacy rights may be compromised due to the perpetuation of prejudiced narratives.

Several strategies have been developed to mitigate this risk in AI systems. To guarantee that training data more accurately represents the diversity of society, diverse and representative data gathering is necessary.

More specifically, biases in the outputs of LLMs can be found and reduced using robust bias detection and correction procedures. To promote responsible use and reduce bias, ethical frameworks and principles may be incorporated into AI development. In order to ensure that LLMs maintain fairness and data protection, collaboration between the government, business, and other stakeholders is also essential. This is because it enables the establishment of industry standards, open practices, and independent audits, which improves trust and accountability in using LLMs.

Current Government and Industry Initiatives and Practices

Although there are currently no laws that regulate LLM in Nigeria, the National Information Technology Development Agency (NITDA) is leading some work in this area through the National Centre for Artificial Intelligence and Robotics (NCAIR) and other stakeholders. This collaboration has given birth to the draft of the National Policy on Artificial Intelligence. In furtherance of this course, NITDA has invited experts to collaborate in developing the National AI Strategy. In the same vein, the UK government has agreed to partner with Nigeria on the security and safety of AI.

BEST PRACTICES IN HANDLING SENSITIVE INFORMATION IN THE ERA OF LLMS

Given that LLMs are trained with data, especially personal data. Users do use personal information in LLM prompts. So it is imperative to ensure the privacy and security of data not just in training LLMs but also while using the generative AI. Personal data can be secured in LLMs by adopting the following best practices:

- **Data Minimisation**

The principle of data minimisation requires that the personal data collected by the data controller/processor is limited to only the relevant data necessary for the stated purpose of processing. Given that it is virtually impracticable to align with this principle since there is a need for a large volume of data to train the LLMs, the end-user of Generative AI must help mitigate the risk attached to training LLMs with extensive data. A profound best practice is limiting the personal data of an end-user in any prompts adopted.

- **Anonymisation**

Where models must learn from sensitive data, anonymisation is a best practice. Anonymisation is the modifying or removing personally identifiable information that may lead to identifying a data subject while maintaining the usability of the data. Although anonymisation is a profound suggestion, it is crucial to note that it does not address the concern of data collection, purpose.

- **Regular Audit/ Penetration Testing**

Similar to testing the security infrastructure of the data storage mechanism, monitoring LLM logs is also crucial to identify the vulnerabilities and mitigate any risk identified.

- **Regular Updates**

For optimum performance and to keep an AI application safe from vulnerabilities, there is a need for constant updates. This responsibility lies more on the end user of the AI tool as soon as a new update is released. This addresses vulnerability issues that may be spotted in an existing application.

- **Ethical Consideration**

Training LLMs has raised ethical considerations on data processing and the risk of data misuse. To address this menace, there is a need to adopt transparency, fairness, and accountability to ensure that data processing in LLMs is conducted responsibly.

RECOMMENDATIONS FOR STRENGTHENING DATA PROTECTION READINESS

First, there is a need for an improvement on the existing data protection law in Nigeria. This is a crucial step to ensure a comprehensive data protection framework in the country. The new provisions will align with international data protection frameworks and address the unique challenges LLMs pose. The updated law would introduce regulations tailored explicitly to LLMs, including guidelines for their use and limitations. It will also establish mechanisms for oversight and enforcement to ensure compliance with these regulations.

By addressing the impact of LLMs on personal data, it would suffice to say that Nigeria is proactive in protecting the privacy rights of Nigerians.

Collaboration between government, industry, and civil society is crucial to ensure comprehensive data protection in LLMs. Establishing common standards that govern the use and handling of personal data in LLMs should be a priority. This could be achieved through joint initiatives focusing on researching, developing, and implementing robust data protection measures tailored to LLMs. It is discernable that the current administration is working to ensure guidelines and regulations that address the unique challenges posed by LLMs, ensuring the responsible use of personal data and enhancing privacy rights; however, issues bothering data privacy should be addressed.

As the country develops its AI Policy and the Data Protection Act, it should consider the unique challenges posed by LLMs and establish tailored regulations.

These regulations should include guidelines for the responsible use of LLMs, limitations, mechanisms for oversight and enforcement, and clear guidelines for their use in various sectors. Collaboration between government, industry, and civil society can also establish common standards and joint initiatives for research, development, and implementation of robust data protection measures for LLMs.

CONCLUSION

As Nigeria continues its digital transformation journey, addressing the evolving challenges posed by LLMs is imperative. By developing holistic legal frameworks, enhancing partnerships, and investing in research, Nigeria can foster its data protection readiness and ensure that the benefits of AI and LLMs are harnessed in a manner that respects individual privacy and societal well-being. The collective effort of government, industry, and civil society is pivotal in shaping a secure and prosperous digital future for Nigeria.

THE ROLE OF STATE AND NON-STATE ACTORS IN DATA PROTECTION

BY

OLANIYAN MARY OMOBOLANLE

INTRODUCTION

Over the past decade, Nigeria and the rest of the world has experienced an astronomical surge in the infiltration of digital technology in almost all aspects of our lives. On a daily basis, millions of individuals utilize the internet for various activities such as, E-Banking, E- learning, online shopping, virtual meetings, use of SNS, etc. In a bid to facilitate easy access and use of these platforms, Internet users and subscribers are required to provide their personal data. With about an estimated amount of 2.5 million quintillion bytes of personal generated in the world daily, personal data is fast becoming of great value to government and private organisations.

It is thus not an overstatement to say that the proliferation of digital technologies has been of immense benefit to mankind and has eased of the stress involved in the traditional and conventional way of handling things. At the same time, IT could pose serious threat to an individual's personal data if not handled properly. This is because the advent of technology has brought about an environment where an individual's data can be accessed, misused and even exploited by anyone if there is no adequate protection of same.

The increasing volume and use of personal data alongside the advent of modern technology enabling new ways of processing and using it has sparked an increase in interest and research into what data protection is and brings about the need for an effective data protection framework to ensure the protection of such data. Data protection has been commonly said to be the law designed to protect an individual's personal data.

Hence, this essay seeks to initiate a discourse around critical issues affecting data protection in Nigeria as well as the role state actors and non-state actors can play to contribute to the full maximization of the Nigeria's data protection space.

ISSUES IN THE DATA PROTECTION SPACE IN NIGERIA.

The journey to developing a comprehensive data protection framework in Nigeria has been a long one with numerous yet unsuccessful attempts to enact a data protection law. Some authors are of the view, that this status quo is as a result of the lack of commitment by the Nigerian government and the absence of a strong political will. Prior to the release of the NDPR by NITDA in 2019, there were several ancillary provisions on data protection in various legislations in Nigeria(list them in footnote). However, presently in Nigeria, what is in place as the extant framework on data protection is the NDPR released by NITDA.

Meanwhile, not to undermine the effects of the NDPR as it actually contains laudable provisions, however a cursory look at the regulation will reveal that it is fraught with quite a number of loopholes and shortfalls hence making it inadequate for the protection of personal data in Nigeria. Besides, the NDPR is a regulation and not a primary legislation.

Knowledge gap amongst majority of the Nigerian citizens is another issue hampering data protection in Nigeria. Most Nigerians do not have sufficient knowledge regarding their rights as data subjects under the NDPR and other relevant legislations that touch on data privacy, thereby making the enforcement of such rights in event of a breach almost impossible. These and many more are some of the issues affecting the data protection space in Nigeria.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

PROSPECTS AND ROLES OF STATE ACTORS AND NON STATE ACTORS IN DATA PROTECTION

In a bid to develop a working data protection ecosystem, all hands need to be on deck to achieve this. Contributions and efforts from individuals, private sector, the public sector, civil societies and even the educational system is highly needed. As earlier stated, this essay will examine how these actors come into play and the significant roles which they can play.

Roles of state actors.

No doubt that the state actors has the most role to play in the grand scheme of things. Top on the list will be to enact a comprehensive data protection law in Nigeria. The enactment of this piece of legislation will go a long way in showing the government's commitment towards data protection and further boost the enforcement drive of data protection issues. At this point, Nigeria needs to be circumspect when doing this and not just enact a pure replica of western laws, instead, these western laws should serve as a guide to enacting a law that will suit Nigeria's peculiarities.

Further, state actors could also act as a catalyst in putting in place a dedicated and independent data protection agency or authority which is free from undue executive influence cannot be over emphasized. There have been positive steps to actualize this especially with the creation of the National data protection Bureau in March 2022, however, it is not just to create an agency but also it is pertinent to ensure the independence of such agency so as to enable it carry out its duties effectively as independence is not just on paper but same is evidenced in deeds and actions.

The independent supervisory authority could adopt, awarding compliant organisations with incentives and rewards so as to boost morale and at the same time mete out stricter penalties to deter noncompliance as reports indicates that there is usually a 30% increase in compliance with the law when incentives are attached.
Another significant role of state actors on Nigeria will be to ratify regional data protection instruments i.e. the AU Data protection convention as well as the ECOWAS Supplementary Act.

The need for the domestication of these instruments becomes very germane, in light of the various cross-border nature of data protection issues.

Roles of Non State Actors.

The NDPR imposes certain obligations on organisations that deals with personal information so as to ensure that an individual's data is lawfully obtained, processed and discarded appropriately. These obligations include the requirement to conduct a data protection audit by organisations that processes personal data of more than 1000 data subjects, development and implementation of a workable, clear and unambiguous privacy policy on the organization's website or at any point of data collection, processing of data should be in line with the lawful basis amongst other obligations.

Compliance with these obligations by organisations will go a long way in developing the desired data protection framework in Nigeria and it is also an avenue for non-state actors to contribute to development of data protection. At the same time compliance by these organisations will also help in sustaining the level of trust between the organisation and their consumers whilst also improving the good will of such organization.

Civil societies and media organisations are also key non state actors and can contribute their quota to the data protection ecosystem by creating awareness about data protection amongst the Nigerian populace. As earlier stated, there is a huge knowledge gap about data protection amongst majority of the Nigerian populace. This is partly due to the fact that there is a lethargic enlightenment towards data protection rights. Civil societies as well as media organisations can be of great help in bridging this gap by creating awareness on digital rights and change the status quo.

In the same vein, Educational institutions are also key stakeholders particularly at the tertiary level. The discourse on human right should be extended to include a discussion on digital rights such as data protection.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Organisations can also undertake a training program for their staffs to properly equip them with the requisite knowledge on how to handle their client's personal data. Judges are also left out and should undergo workshops and seminars on data protection and how to properly address and adjudicate on cases relating to same.

CONCLUSION

Data protection has gotten to a level where it is global concern and a topic to various actors. It is now everyone's business hence, a lot of joint efforts is thus required not only from state actors only, but also from non-state actors as well as other relevant stakeholders in guaranteeing that the data protection space remains up to data so as to meet up with the latest trends of the digital world.

THE ROLE OF STATE AND NON-STATE ACTORS IN DATA PROTECTION

BY
OLUWADAMIPE

BACKGROUND

Data is an integral part of governance, trade and commerce, and security. It is vital for efficient decision-making at policy and programmatic levels and grassroots, as it has now been identified as a crucial factor for policy success. In an age where institutions now depend heavily on data, data protection has become a priority. This includes its entire process from creation or acquisition to utilisation and evaluation. At micro level, data protection of individuals is now a right, as it is a proven element of human security. Overall, the place data holds in society and the rationale for protecting is the backdrop upon which one may argue that state and non-state actors play vital roles at different levels, as a multi-stakeholder approach is best suited for effective data protection. While data is a collection of values expressing quality, quantity, facts, statistics etc., data protection may be understood as protecting data, its composition, related systems and infrastructures from misuse, alteration, corruption, interruption, misdirection, deletion, theft, damage or unauthorised access or processing. It is about safeguarding data from all forms of compromise, while simultaneously ensuring its availability for use when needed by authorized parties, for intended purposes. Summarily, therefore, guarding the availability, confidentiality and integrity of data is the essence of data protection.

Data protection has the attention of various users and stakeholders with various agenda, at different levels and with varying categorization. At the root of this is the frequency at which data is communicated and the increasing level of their dependence on it. Data has emerged as one of the most important assets to organizations in this digital age. As such, its protection is non-negotiable. The benefits include- ensuring the safety, personal integrity and financial security of individuals, protecting vital data of government institutions from malicious use and fraudulent activities and protecting organizations from the debilitating financial implications of a data breach or cyber-attack. This additionally promotes the goodwill and reputation of brand owners, by building the trust of customers.

Within the context of this piece, states are political sovereign entities that possess the legal and legitimate authority over an area of territory and the people in it. 'Actors' in the context of this work, are players that have the capacity to impact societal policy and the capacity to possess an agenda, or follow that of another at local and international levels. While non-state actors do not possess any sovereign power like state actors, they have the capacity to influence policy processes.

Data protection involves protection at three main levels: political, technical, and legal; and their interplay in the world today demonstrates that each level impacts the others, to the benefit or detriment of the users and stakeholders of the data in question. The political aspect has to do with policy making and implementation. The technical aspect concerns itself with the technical means and methods of data protection, while the legal aspect is about law making and implementation and the legal system or regime that ensures data protection regardless of political or technical restraint.

ROLE OF STATE AND NON-STATE ACTORS: AN OVERVIEW

From a legal perspective, the role of state actors in the legal aspect of data protection relates to the enactment of laws for the protection of data. Law making is a key function of state actors. State actors are tasked with the development of a legal framework for data protection within their respective territories. This Legal framework would comprise standards of data protection for institutions and stakeholders, regulatory sanctions for violations as well as procedures for seeking redress. This would be executed on a National level. Also, under the Legal aspect of Data protection, state actors have the responsibility for ratifying and implementing International Legal instruments for the enrichment of data protection in their territories. In the European Union, such an instrument is the European Union General Data Protection Regulation. In Africa, the African Union Convention on Cyber security and Personal Data Protection exists. Once ratified by individual state actors within their territories, such laws become operational for guiding the conduct of the relevant institutions and stakeholders with respect to data protection. Execution however, may require an implementation roadmap.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Non-state actors as well, have significant roles to play in the Legal aspect of Data protection. This is with respect to their unofficial oversight functions. They act as watchdogs to ensure careful implementation of enacted laws and, review with the aim of repeal of obsolete ones. Furthermore, they can assist state actors in monitoring and evaluation of policies, which is useful for evaluating impact, identified gaps and opportunities.

The technical aspect of Data protection is the operational/functional aspect of data protection mechanisms. Here, the role of state actors is to ensure the implementation of enacted legislation by the development of implementation road maps. It is not sufficient to have brilliant laws. The impact of such laws is seen in their effective implementation. Therefore, the formulation of strategy by which enacted laws will be executed is a role of state actors. In light of this, state actors are tasked with the creation of National data protection authorities to oversee the compliance of individuals and institutions with Data protection laws. Along with this, regulatory institutions as may be expedient for this task, may be established with responsibility for monitoring of and response to data protection incidents, advisory functions, alerts in cases of violations etc. Equally beneficial would be guidelines delineating the roles of law enforcement agencies and the modus operandi for collaborations between regulatory agencies and law enforcement agencies. Where these regulatory agencies exist, they must be adequately supplied with the financial, technical and human resources needed to carry out their objectives. The execution of this role is both at the National level and regional (component units) levels for greater effectiveness.

Furthermore, state actors are tasked, under the Technical aspect of Data protection, with the development of relevant programs and initiatives to promote Data protection. This could take the form of public-private partnerships with companies and individuals that are equipped with the technical know-how, to promote technical education for information and communication technology professionals, through certification and standardization of training; categorization of professional qualifications as well as development of needs-based distribution of educational material. The Technical roles of Non-state actors in Data protection include responsibility for educating the public on the meaning, merits, methods and laws of Data protection. Non-state actors could undertake enlightenment and education campaigns from the grassroots to the National level. The benefit of this is its likelihood of promoting wilful compliance with laws.

Proper understanding of the intent and benefits of data protection legislation by the public and relevant stakeholders should result in higher compliance levels and reduced exertion by regulatory agencies. An additional role of Non-state actors in this Technical aspect is promoting data protection by encouraging and influencing large organizations to commit resources towards the acquisition of data protection tools and equipment for small and medium scale enterprises. This includes financial donations, sponsored workshops etc. The execution of this role is on global (multinational organizations) and national (indigenous organizations) levels.

Furthermore, Non-state actors' adhere to policy and legal framework for data protection (especially businesses) and give feedback to the relevant authorities. They are also required to ensure that consumers of their products are adequately informed with relevant knowledge. Lack of knowledge and awareness undermines data protection.

The third aspect of Data protection is the political aspect which relates to policies and policy-making processes. Policies are principles; proposed courses of action to be implemented by a governing body. State actors are the policy makers. Thus, their role in the political aspect is the promotion of a culture of data protection and data compliance by the establishment of significant policies. For instance, to encourage compliance with data protection laws, state actors could give fiscal concessions to compliant organizations. Additionally, state actors could make policies guaranteeing stakeholder participation in law-making processes. Adequate communication between the law-makers and stakeholders could result in the enactment of laws that are industrially relevant and readily acceptable. Compliance would not be an endless tussle between agencies and stakeholders. Non-state actors have been known to influence the decision-making process and policies of State actors. On this aspect, through advocacy, research and consultations they could band together to develop policy recommendations and innovative ideas of implementation to enhance the state of data protection in their respective countries.

CONCLUSION

Data protection has emerged as non-negotiable to individuals, organizations and governments of the twenty first century. Its weakness or absence in legal, technical and political terms have impacts on the security and rights of humans. In this regard, the role of state and non-state actors at the different levels (legal, political and technical) and their interaction is important. Furthermore, the roles at international, national and local levels are complementary to enhance data protection for the benefits of all.

THE ROLE OF STATE AND NON-STATE ACTORS IN DATA PROTECTION

BY

ABDUL PELUMI GANIYU

Introduction

Yahoo was at its peak as the global most valuable company in 2000. However, within the year 2013 and 2014, the company lost over 350 million dollars due to data breaches on two occasions -first in 2013, where over 3 billion personal records leaked and the other in 2014, where another 500 million personal records was exposed-. This damaged the brand immeasurably and forced it to lower its estimated 680 million dollars sale price to 350 million dollars. The downturn of this event among others further put governments and several sectors on their toes in participating and contributing to data protection.

What is data protection?

Data protection is the process or a strategy that involves safeguarding significant information from loss, compromise or corruption and securing the integrity, availability and privacy of data while keeping it usable.

For every organization, the centre of attention and business is data. Data is significant and essential in response to unforeseen events, market shifts and in meeting the needs of customers. Therefore, data protection needs to always be on the mind of enterprises as billions of personal information are shared by people (particularly customers) online while purchasing digital services and consuming contents. That is, the growing volume of personal data -names, email address, phone number and credit card details among others- shared means a gross increase in cyber attacks, threats and data leaks, corruption and theft.

Thus, the importance of data protection cannot be overlooked as it helps in availability, confidentiality and integrity of data stored within an organization. Unlike data privacy that defines only those who can access data, data protection further covers policies and tools in data access restriction. This is why globally there exist principles of data protection compliance that are in correlation with the standards set by the European Union General Data Protection Regulation (GDPR) 2018.

Who are the State and Non-State Actors?

Simply put, state actors are governments of countries or government representatives acting in official capacity. On the other hand, non-state actors are organizations including individuals that do not have a direct link or affiliation or are funded by any governments and most times exercise territorial or political influence. Examples of non-state actors are Non-Governmental Organizations (NGOs), private financial companies and corporations from others.

Hence, the difference between a state and non-state actors is that the former are the governments and the latter are individuals or private institutions that have the potential of influencing governmental decision or action.

The Role of the State and Non-State Actors

To begin with, one of the primary obligations of a state actor is the security of the people of the state. Today, the world is gradually progressing into the fourth industrial revolution, characterized by digitization. As a result, the issue of state security extends to data security (protection) as personal information is shared via the internet, which makes it open to abuse.

There is a need by governments to collaborate with the necessary bodies at the domestic level and internationally -as data is shared beyond borders, same as cybercrimes- in passing and enforcing comprehensive and effective data protection laws. Where there are legislative standards in place for data protection, rights of individuals to control and access their personal data should be clearly identified.

Another role of governments is to limit the use of biometric data by private companies and government institutions. Biometrics -DNA profiles, hand geometry, voice, face, fingerprints and others- are always subjected to high personal security and privacy threats, especially where there is a weak legal framework for data protection. For instance, more than 28 million biometric data (passwords, facial recognition token and fingerprints) was stolen in 2019 at the UK biometrics provider. Hence, governments need to limit the access and use of biometrics by private companies to only small groups and this may be through strong regulations or policies.

Non-state actors, particularly companies or private institutions that procure personal data should always ensure to enforce a runtime encryption of data stored in their server or hard drives. Also, companies need to implement a strong security network and run a routine check of firewalls to detect anomalies or threats in their software network. Since hackers do find a way around biometric authentication, the use of anti-spoofing technology with live detection would aid in blocking unauthorized access to biometric data.

In addition, non-state actors such as Non-Governmental Organizations (NGOs) and civil societies need to start creating awareness, monitor government policies and advocate alternative policies in appropriate cases on data protection. This is because only about 66% of the world population have laws on data privacy and protection and in America alone, over 67% of its population are not aware of any law on data protection and privacy.

Therefore, non-state actors are to focus on creating awareness on data protection by educating individuals on the intricacies of data protection, introduce them through civic engagement to key laws, regulations and policies on data protection and offer them guides on how to use the internet effectively so as to avoid unnecessary sharing of personal information.

Moreover, state actors need to restructure the use of mass surveillance by ensuring that surveillance is targeted and not general with strong judicial oversight, where the people can challenge the same. Although, surveillance is usually authorized particularly by the use of technology in generating data or monitoring communication of persons suspected of wrongdoing or to prevent crime. However, the use of mass surveillance makes it easier for government and law enforcement agencies to indiscriminately access personal information of people, infringe on their privacy rights and impliedly control them.

Limiting mass surveillance to targeted persons or with a court order would help protect data of citizens from being exposed to inappropriate use by governments or other persons that might lawfully or unlawfully access such data. And for states with bilateral agreement on intelligence sharing and surveillance such as the Five Eyes, constraints and measures provided for the state should be made applicable internationally in order to prevent double standards.

Lastly,there must be a combined effort between the state and non-state actors towards combating cyber-attacks, which is the major driver of data breaches. According to statistics, there has been a global increase in cyber-attacks by 125% throughout 2021 and is moving upward in 2022. This has caused an increase in the rate of data breaches as victims of data breaches moved from 6 in 2001 to 97 per hour within the last two decades (a 1517% increase). Moreover, a report from the Ponemon Institute showed that data breaches cost 4.35 million US dollars so far in 2022.

Premise on this, state actors need to collaborate with non-state actors both nationally and internationally in providing the necessary strategies and comprehensive legal framework for cyber-security and in providing the appropriate punishment for cyber-criminals cross jurisdiction. Also, state and non-state actors need to work together in implementing suitable and effective technologies in providing a secure cyberspace. This includes adopting the best smart technologies such as cloud computing, artificial intelligence, internet of things (iot), social engineering, firewalls and Data Loss Prevention (DLS) and intrusion detection and prevention systems from a host of others.

Conclusion

The role of state and non-state actors in data protection can not be overlooked. This is because apart from individuals taking the necessary steps in protecting their personal information, governments and institutions including private companies have a critical responsibility to undertake as regards data protection. This is why this paper clearly identified the role expected of state and non-state actors ranging from strong legislative frameworks, awareness and education to combined efforts towards combating cyber-attacks on data protection. It is axiomatic that if the roles are implemented, there would be a new world order, where data is highly safeguarded, secured and protected. Now is the time to make the role of state and non-state actors in data protection a reality.

THE AFRICAN UNION 2063 AGENDA AND DATA PROTECTION

BY

GABRIEL OMONIYI

ntroduction

The General Data Protection Regulation ("GDPR"), which entered into force on 24th May 2016 (but became applicable on 25th May 2018) has remained a model for the regulation of data protection globally. Although there are other legislations like the California Privacy Rights Act, United Kingdom Data Protection Act 2018, etc. which have been equally enacted in other countries, the direct application of the GDPR to all the European countries has rightly placed ahead the GDPR as being revolutionary with its wide acceptance and uniformity of rules across the member states in the European Union ("EU"). Significantly, the provisions of the GDPR on relevant provisions which guarantees the rights of data subjects, the regulation of cross-border transfer to third countries or international organisations and the obligations of data controllers and processors have reinforced the primacy of data protection and elevated the data subjects as "kings" in the EU.

Coming home to Africa, the regulation of data protection is still in a nascent stage when compared to Europe. More importantly, the lack of uniformity in the laws (or lack of laws and regulatory institutions in some African countries) and a continent-wide institution with direct and administrative competence like the EU and its organs can be deemed a factor that has possibly stalled the development of data protection, amidst other relevant policies and institutional developments in Africa. Realising the back-seat position Africa has taken when compared to other continents, the African Union ("AU") on its 50th anniversary in 2013 has set an ambitious 50-year project tagged – "African Union 2063 Agenda" ("Agenda"). The Agenda will entail the "mobilization of the people and their ownership of continental programmes at the core; the principle of self-reliance and Africa financing its own development; the importance of capable, inclusive and accountable states and institutions at all levels and in all spheres; the critical role of Regional Economic Communities as building blocks for continental unity; taking into account of the special challenges faced by both island and land-locked states; and holding ourselves and our governments and institutions accountable for results."

This essay will therefore examine the past and recent efforts of the AU in regulating data protection, together with the future and practical steps that can be taken to improve the regulation of data protection in Africa, most especially towards the actualisation of the aspirations set out in the Agenda.

The Past and Recent Efforts of the AU and Member States on Data Protection

The discussion on data protection cannot be outrightly said to be new in Africa given that there have been legislative or policy instruments either at the AU level or in some member states for about a decade. At the AU level, there has been the African Union Convention on Cyber Security and Personal Data Protection ("Convention") which was adopted on 27th June 2014 and some regional and national laws on data protection like the Economic Community of West African States Data Protection Act 2010, the South African Protection of Personal Information Act 2013 and the Nigerian Data Protection Regulations 2019 ("NDPR") just to mention a few. Aside from these primary legislative texts, there have been some other secondary texts and policy documents like the AU Data Policy Framework ("Framework"), the Interoperability Framework on Digital ID, the Declaration on Internet Governance and Development of Africa's Digital Economy of 2018, Personal Data Protection Guidelines for Africa ("Guidelines"), etc. which have been issued by the AU and some in conjunction with some other entities to equally regulate data protection and technology in Africa.

The Convention, being a treaty, sets its objective *inter alia* to strengthen "fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle to free flow of personal data." Chapter II of the Convention is centred on data protection with provisions on the institutional framework for the protection of personal data, obligations relating to conditions governing personal data processing, the data subjects' rights and obligations of the data controller. Sadly, the Convention till date has only been ratified by 13 member states of the 55 countries in Africa.

I

In 2018, the Guidelines, a joint initiative of the Internet Society and the Commission of African Union was issued. The Guidelines set out eighteen recommendations with the aim to serve as a blueprint for an evolving process of developing policy, operational guidelines, and best practice. Some of the recommendations include the expectations from relevant stakeholders like the governments and policymakers, data protection authorities, data controllers and their partners etc. The successful implementation of this Guidelines is in doubt given that it lacks a force of law and serves only as a guide to the member states of the AU.

More recently, the Framework issued in 2022 has set out some important policies that should regulate data protection in Africa. The Framework sets out its objectives to provide "principle-based guidance to member states in their domestication of the continental data policy appropriate to their conditions and proposes a continental instrument or mechanism to integrate and coordinate continental efforts" and "strengthen national data systems for effective use of data by creating an enabling environment that stimulates innovation and entrepreneurialism to drive the development of data value-driven economies and that facilitates the interoperability of systems and cross border data flows necessary for the realising of the African single digital market" The recency of this Framework, however, makes it difficult to assess the successful implementation of the suggestions contained therein.

It is instrumental to note that despite these attempts of the AU and the member states in regulating data protection, the continent has fallen prey to data misappropriation and has been unable to stand its ground like its EU counterpart. A copious example is the Facebook-Cambridge Analytica scandal wherein it was found that the election results in Nigeria and Kenya (2013 and 2017) were manipulated using private data from the Facebook account of their citizens for private messaging.

The Future and Practical Solutions to Data Protection in Africa

An in-depth review of the Agenda has revealed that although there is no specific mention of data protection in the Agenda, Aspiration 3 – an Africa of good governance, democracy, respect for human rights, justice and the rule of law and particularly in paragraph 28 makes provision for the universal principles of human rights (of which data protection can be subsumed) and the establishment of competent, professional, rules and merit-based public institutions that will serve the continent and deliver effective and efficient services can interpreted broadly to accommodate the principles on data protection in its paragraph 30.

either be revised by a Protocol to the Convention or a new treaty signed to properly reflect the current issues in data protection. Topical issues like the cross-border transfer of data to third countries and international organisations, innovative practices like binding corporate rules for large corporations in Africa, the establishment of a regulatory body at the AU level and applicable penalties to defaulting individuals (both personal and corporate) should be properly addressed. Equally, the rights of the data subjects as contained under the Convention should be expanded and well-detailed to accommodate the right to restriction of processing of data and data portability while necessary obligations needed to drive top-level compliance with the principles of data protection are imposed on data processors like it is done under the GDPR.

In addition, the AU should through partnerships with the relevant national bodies and non-governmental organisations organise programmes that will sensitise Africans on the importance of data protection. This will help create self-awareness in the mind of Africans in dealing with data-gathering platforms and inform them of the avenue created by the laws to approach the regulatory authorities and judicial bodies for enforcement of their rights in case of infringement and claim for monetary compensation.

Equally, the success of the African Continental Free Trade Agreement (AfCFTA) in ensuring free trade of goods and services may, as noted by the Mandela Institute at the University of Witwatersrand, Johannesburg ("Institute"), be affected in light of some data protection laws and regulations which may limit the cross-border flow of data with various unintended consequences. While this may be justified in light of the concerns further raised by the Institute to include protection of personal data, access to data by local law enforcement, ensuring national security, advancing local economic competitiveness and levelling the regulatory playing field, the resultant effect on the long run is that free trade will be heavily impacted, transaction costs increased, the efficiency of corporations affected, innovation stifled and economic growth hampered. Given the importance of the AfCFTA in Africa and at this time, the lack of adequate legislation on data protection should not be the hindrance to the full maximisation of the AfCFTA.

Conclusion

Given the above analysis, the AU, with the aspirations and steps set out for Africa in the Agenda, seems to be on the right track of development. The wake of technological advancements and widespread adoption of technology across almost all the sectors has raised a new need and challenge of data gathering hence the need for appropriate protective measures. Beyond the fine prints in the Agenda, the AU must understand the power it can wield to provide for adequate data protection legislation and policies that can combat possible misappropriation of data. Conscious efforts must therefore be made to enact an all-encompassing legislation that will guarantee a uniform application of data protection laws in Africa, provide the citizens with realistic and hassle-free enforcement procedures for their rights and ensure there are guarantees for cross-border data processing activities.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

THE AFRICAN UNION 2063 AGENDA AND DATA PROTECTION

BY
AYODEJI AYOOLA

Abstract

Data protection is now a priority, whether the African region likes it or not. The Agenda 2063 has served as a foundation for the introduction of various programs and projects which impact data protection within the region, whether directly or indirectly. Therefore, in light of the Agenda 2063, this essay examines the progress of data protection in the African region. Using literature review and official documents issued by the African Union (AU) and other international bodies, this essay hopes to raise awareness about the interesting facts that shed light on the current status of data protection in the African region, while considering the Agenda 2063. The essay is written in 3 parts. Part 1 gives an introduction to the Agenda 2063 (its aspirations, aims and objectives) and sheds light on its connection to the subject of data protection in the African region. Zeroing in on data protection, Part 2 assesses the progress of data protection under the Agenda 2063 50-year regime by evaluating one report, one international agreement, and one international policy document. This evaluation gives momentum to part 3 which briefly concludes the essay with a few recommendations on how data protection goals can be achieved in the African region alongside the broad objectives of the Agenda 2063.

Keywords: Africa; African Union; Agenda 2063; Data Protection; Cybersecurity.

PART 1

The essay begins with a review of the creation, purpose and contents of the Agenda 2063. This introduction sets the tone for a discussion on the impact of regional integration agreements on economic factors which then impact data protection directly or indirectly. It is however assumed that the concepts of cybersecurity and data protection are essentially similar and univocal – connoting the protection of (personal) data. This assumption is necessary because this essay highlights a few cybersecurity projects/programs in the African region which are noteworthy for discussing the subject of data protection.

Agenda 2063 and Data Protection – the Link

Agenda 2063 is a 50-year strategic framework with the primary goal of directing Africa's development for the ensuing half-century and realizing the vision of The Africa We Want. The goal of Agenda 2063 is to serve as Africa's master plan and blueprint for transforming the continent into the future global powerhouse. In addition to being a tangible expression of the pan-African drive for unity and progress, it is the continent's strategic plan for achieving inclusive and sustainable development.

Generally, regional integration agreements have an impact on cross-border transfers of personal data, online transactions (trade), and people living and working in member states other than their country of origin. They also have an impact on standardizing, protecting, and respecting the privacy of identity data of citizens. This explains how regional integration and data protection are related. The AU member states have a responsibility to ensure that regional integration, free trade, and development are not hampered or made more dangerous by the inability to exchange personal data in a way that is appropriate, secure, and respectful of people's rights. Additionally, the emergence of digital technologies and the rise in popularity of web-based platforms are rapidly altering how people, organizations, and governments all over the world conduct business. For instance, 60% of people in Africa use their mobile devices to access the Internet.

However, in addition to agreements for regional integration, the Agenda 2063 has also served as a framework for the introduction of initiatives that have an impact on data protection in the region, either directly or indirectly. In the middle of the 20th century, when many African nations gained their independence, there was a "cry" for economic stability all over the continent. Through international insertion and development strategies, this resulted in the formation of political and economic alliances. Agenda 2063, which received the support of the African Heads of State and Government in January 2015 at the 24th Ordinary Session of the Assembly of the AU, aims to ensure that Africans have adequate living conditions while also fostering a new political and economic integration into the global system. In a nutshell, the ability of AU member states to realize the goals and objectives of Agenda 2063 is crucially enabled by a safe, reliable, and privacy-respecting data regime.

Is Data Protection a priority under the African 2063 Agenda?

The AU probably did not have data protection in mind when it created Agenda 2063. Examining the Agenda 2063 document reveals that "cybersecurity," "data protection," and "data privacy" were not specifically mentioned. The AU, however, has gradually given it serious consideration. Through the development of the "flagship projects" under the First Ten Year Implementation Plan, the specific inclusion of cybersecurity as a distinctive goal under the agenda was started (FTYIP). The first of five ten-year plans over the fifty-year horizon of Agenda 2063's 50-year time frame is the FTYIP (2013-2023). The term "flagship projects" refers to important initiatives and programs that have been identified as essential to accelerating Africa's economic growth and development as well as to fostering our shared identity by honouring our rich cultural heritage. Making cyber security the centrepiece program of Agenda 2063 is a glaring indication that Africa needs to not only account for the rapid changes brought about by emerging technologies in its development plans, but also to ensure that these technologies are used for the benefit of African people, institutions, or nation-states by ensuring data protection and safety online.

A more definite reference to the term “data protection” and “privacy” was in 2018 when the Privacy and Personal Data Protection Guidelines for Africa (“the Guidelines”) was drafted. The Guidelines (developed by the Internet Society (ISOC) upon the AU’s request) were premised on paragraph 31 of the CCPDP which mandated the AU to develop guidelines on personal data protection.

PART 2

This part provides a status report on the progress of data protection in the African region under the Agenda 2063 50-year regime. This builds the momentum for part 3 which makes a few recommendations. It is noteworthy, however, that quantifiability is a challenge to assessing progress in data protection goals. Even African nations face significant obstacles when trying to make the development agenda's targets measurable and building the statistical capacity needed to gather the data needed to measure those targets.

Progress of Data Protection in the African region under the Agenda 2063 50-year regime

To facilitate the discussion under this Part, reference will be made to one report, one international agreement, and one international policy document – as follows:

1. First Continental Report on the Implementation of Agenda 2063

In the First Continental Report on the Implementation of Agenda 2063, cybersecurity is mentioned as one of the flagship projects of the Agenda, and a status report is provided. According to the report, the primary goal of the cybersecurity project was to ensure that by the year 2020, the digital economy will account for nearly one-third of the total global gross domestic product (GDP) . In February of 2020, however, only 4 of the required 15 member states had ratified the CCPDP. It further stated that several African nations are still in the early phase of developing their cybersecurity legal and regulatory framework. Most of the data protection laws of member states seem to place more emphasis on protecting businesses' bottom lines than on shielding people from harm. Also, most of the laws were modelled after their European counterparts. In addition, while acknowledging that the project's lack of budgetary resources has delayed its implementation, the report recommends resource mobilization to develop the continent's capacity building for cybersecurity.

1. African Union Convention on Cybersecurity and Personal Data Protection (CCPDP)

The African Union Convention on Cyber Security and Personal Data Protection (CCPDP), sometimes referred to as the Malabo Convention, was approved by the AU members states in 2014. The Declaration established a clear and ambitious goal for “African action on cybersecurity and the protection of personal data” . The Convention offers a road map for directing the various cybersecurity projects that have emerged from Agenda 2063. Within the realm of cybersecurity, the CCPDP addresses the following three primary areas: (1) electronic transactions; (2) protection of personal data; and (3) cybersecurity and cybercrime.

The protection of personal information is covered in detail in Chapter II of the Convention which is broken down into its three primary sections.

The first section deals with the protection of personal data in a general sense; the second section highlights the institutional framework for the protection of personal data; and the third section lays out the fundamental principles that govern the processing of personal data and the rights of data subjects. However, because the CCPDP has not been ratified by the majority of African states, its impact on the continent has not yet been significantly realized.

1. **The Privacy and Personal Data Protection Guidelines for Africa (PPDPG)**

The Privacy and Personal Data Protection Guidelines for Africa (PPDPG) ("the Guidelines") were developed by the Internet Society (ISOC) upon the AU's request. The development of the Guidelines took place against the backdrop of ambitious policy goals for Africa as outlined in Agenda 2063, as well as against the backdrop of fast change in the scope and availability of online services in Africa. The Guidelines emphasise the significance of ensuring trust in online services as a critical component in the maintenance of a productive and advantageous digital economy. In addition to this, they provide direction on how to assist individuals in taking a more active role in the security of their personal data, while at the same time acknowledging that beneficial outcomes for individuals depend, in many areas, on positive action taken by other stakeholders. The usefulness of the Guidelines is, however, open to debate seeing that they are unenforceable and not binding.

Part 3

Leveraging on the discussions in Parts 1 and 2, this final part concludes the essay with a few recommendations on how data protection goals can be achieved alongside the broad objectives of the Agenda 2063.

Conclusion and Recommendations

A more consistent approach is required for the creation of regulatory bodies and other enforcement mechanisms across the African region, as well as a greater need for consistency in the protection of personally identifiable information across the continent. In order to facilitate the transfer of personal data across international borders in the African region, the member states have a responsibility to develop criteria that are both standardized and consistent with one another. In the context of assessing performance information in the domain of data protection across the African region, monitoring and evaluation systems also play an essential role. It's possible that the African Union (AU) needs to learn the practice and culture of monitoring and evaluation, which are deeply ingrained in organizations like the United Nations, the World Bank Group, and the OECD.

What is more? It is in the best interest of subregional organizations to encourage and ensure that all their members adopt and adhere strictly to the tenets designed to enhance their development. A proper step in this direction is that the AU persuades all the remaining member states to sign the CCPDP. Sanctions may be imposed on erring member states. Even though most of the programs are voluntary, the idea of sanctions could persuade states that have not previously been willing to cooperate with AU's development platforms. In the realm of data protection, this will contribute to the enhancement of continuity in the African Union's development programs for the continent.

THE AFRICAN UNION 2063 AGENDA AND DATA PROTECTION

BY

OLAWOYIN MUSTAPHA TOLANI

INTRODUCTION

The vision of the African Union is to create an integrated, prosperous Africa, driven by its own citizens and representing a dynamic force in the global arena. To achieve this vision, the African Union developed some frameworks, most of which are subsumed under the Agenda 2063, to develop the continent into a global powerhouse. For instance, the African Continental Free Trade Area (AfCFTA) Agreement being one of the frameworks is a trade agreement by member states of the African Union which seeks to foster inter-African trade through deeper levels of trade liberalisation and enhanced regulatory harmonisation and coordination. The African Continental Free Trade Area (AfCFTA) Agreement is one of the flagship projects of Agenda 2063 and it aims at creating a single African market to guarantee the free movement of persons, capitals, goods, and services. This implies that more transactions on goods and services are bound to happen between African businesses than ever before. Consequently, it signifies an unprecedented amount of personal data transfer between these businesses and government entities.

AU AGENDA 2063: A BACKGROUND

The continent is blessed with nature's gift of abundant earthly resources (like gold, crude oil, diamond, timber, iron ore, cocoa, cobalt, platinum, uranium, etc) and a booming human capital. According to the United Nations Environment Programme (UNEP), Africa houses about 30% of the world's mineral reserves, 8% of the global natural gas, 12% of the world's oil reserves, over 40% of the world's gold, about 90% of global chromium and platinum. It also prides itself as host to the largest reserves for cobalt, diamonds, platinum, and uranium.

Despite all the above beaming global track records, Africa is still considered the poorest continent on earth. The content is plagued with myriads of developmental challenges hindering its potential of becoming a global powerhouse. Consequently, the African Union, in a bid to transform the continent into a fantasy of other continents, came up with the Agenda 2063. The Agenda 2063 is a framework that contains a number of transformative aspirations which the continent hopes to have achieved by 2063.

The African Union describes it as "Africa's blueprint and master plan for transforming Africa into the global powerhouse of the future. It is the continent's strategic framework that aims to deliver on its goal for inclusive and sustainable development and is a concrete manifestation of the pan-African drive for unity, self-determination, freedom, progress and collective prosperity pursued under Pan-Africanism and African Renaissance".

The Agenda 2063 contains seven (7) aspirations identified to push the continent's developmental plan into a force to be reckoned with globally. They aspirations are:

Aspiration 1: A prosperous Africa based on inclusive growth and sustainable development

Aspiration 2: An integrated continent, politically united and based on the ideals of Pan-Africanism and the vision of Africa's Renaissance

Aspiration 3: An Africa of good governance, democracy, respect for human rights, justice and the rule of law

Aspiration 4: A peaceful and secure Africa

Aspiration 5: An Africa with a strong cultural identity, common heritage, shared values and ethics

Aspiration 6: An Africa, whose development is people-driven, relying on the potential of African people, especially its women and youth, and caring for children.

Aspiration 7: Africa as a strong, united, resilient and influential global player and partner.

WHAT IS DATA PROTECTION?

Personal Data or Data is any piece of information, either alone or in addition to other information, that can be used to identify a living individual. According to the African Union Convention on Cybersecurity and Personal Data Protection, personal data is "Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental economic, cultural or social identity." Hence, any piece of numeric, alphabetic, or alphanumeric information sufficient to identify a human qualifies as personal data and is subject to protection. Flowing from the above, data protection is therefore the safeguard from abuse and/or misuse of any information capable of being used for the purpose of identifying a person.

THE NEED FOR DATA IN THE REALISATION OF AU AGENDA 2063

Technology has proven to be an important ingredient for the economic development of any nation. The increasing access to different technologies and the internet as a whole in Africa is becoming a catalyst for international trade, commerce, and investment in the light of Agenda 2063. The number of internet users in the continent continues to surge and as a result, internet/tech-based innovations, inventions, products, and solutions are being developed in the continent. As at the first quarter of 2020, there were over half a billion internet users in Africa. The image below also shows a progressive number of internet users in some selected African Countries as at January 2022.

[Fig 1: Number of internet users in selected African countries. Source:Statista https://bit.ly/3trH2qp]

In line with the AU Agenda 2063, the increasing level of tech and innovative solutions plays a key role in the continent's integration. This is because most tech-enabled businesses are beginning to expand beyond their host countries and to other parts of Africa. For instance, Flutterwave is a Nigerian payment platform that is now operational in Ghana, Tanzania, Kenya, and other African countries. The same applies to Jumia, MFS Africa, Chippercash, among a list of other tech-powered businesses engaging in cross-border transactions.

The rapid adoption of technology in Africa is fueled by the availability of data. Most technological innovations require a good amount of personal data to process so as to achieve their potential. This is why data is regarded as the oil that greases the machines of digitalisation.

The interconnectedness of African businesses and organisations envisaged by the Agenda 2063 will result in gazillions of cross-border data transfers. In its sense, this appears to be a good deal for the development of the continent, however, the natural concern for cross-border data transfer of this nature is with the abuse and misuse of personal data. Who then is the Agenda 2063 proposing to protect the personal data of over 1.2 Billion Africans from being mismanaged, abused, misused, or used for purposes other than disclosed.

AGENDA 2063 AND THE DATA PROTECTION CONCERNS

If the 'Africa we want' is one powered by the technology in driving innovation, achieving socio-economic development, and generally turning Africa into a continental village, then as Africans, we must be willing to provide our personal data for the collective good. However, parting with personal data doesn't seem to be the problem for many, the issue lies in the adequate safeguard and protection of the data. The Facebook-Cambridge Analytical's data scandal is a concise instance of how personal data can be misused.

The Convention on Cyber Security and Data Protection is an important framework in addressing the data protection concerns of the Agenda 2063. The Convention, also known as the "Malabo Convention", is a continental regulation passed at the 23rd Ordinary session of the African Union in 2014. It substantially caters for the rights and protection of the personal data of data subjects by the data controllers. Article 13 of the Convention provides for some principles that data controllers must abide by in dealing with personal data of data subjects. The first principle under the Article addresses the issue of consent as it provides that "processing of personal data shall be deemed to be legitimate where the data subject has given his/her consent." The second principle which is also as important touches on the lawfulness and fairness of personal data. This presupposes that personal data collected from data subjects must be processed, stored, and transmitted in a lawful, fair, and non-fraudulent manner. Closely related is the principle of purpose and storage which protects the data subject's data as it relates to specificity of usage and period of storage. Other duties imposed on a data controller by virtue of this Article are regarding the accuracy of data, transparency, confidentiality, and security of data processing. Furthermore, the convention also specifically endows a data subject with a number of rights which includes: the right to information about his data, right to access to his data, right to object to the processing of his data, and right to make corrections to his data or outright erasure.

Another framework is the Personal Data Protection Guidelines for Africa developed by the joint initiative of the Internet Society and the Commission of the African Union in 2018. The Guideline basically appraises the Malabo Convention while briefly examines the responsibilities of major stakeholders like the Government, Policy makers, Data Protection Authorities, Data Controllers, Citizens and Civil Society.

CONCLUSION AND RECOMMENDATION

Against the above backdrop, it can be observed that theAgenda 2063 would achieve little success in the absence of technological innovations. Since personal data has proven to be an important element in technological development, concrete measures must be put in place to ensure its protection. It is recommended that all the regulations, conventions, and guidelines passed by the African Union are harmonised into a single framework for ease of adoption and enforcement. It is one thing to pass a regulation and another to enforce, the African Union is therefore advised to create monitoring, enforcement and compliance measures to ensure that the data protection regulations are effective. It is further recommended that African Union creates a singular regulatory agency for the protection of personal data in view of the Agenda 2063.

THE RELATIONSHIP BETWEEN DATA PROTECTION AND OTHER HUMAN RIGHTS IN NIGERIA

BY

DORCAS TSEBEE

Introduction

Data protection has evolved into a matter of both national and international importance, reflecting the growing dependence of modern economies on the processing of personal data. The increasing use of digital technologies and online services has amplified the risks associated with unauthorised access, misuse, and disclosure of personal information. At its core, data protection concerns an individual's ability to control who has access to their personal information and how it is used.

Inadequate protection of personal data can adversely affect a range of human rights, including the rights to privacy, freedom of expression, non-discrimination, association, liberty, and human dignity. These rights are fundamental to the human person and are recognised under Chapter IV of the Constitution of the Federal Republic of Nigeria 1999 (as amended) ("the Nigerian Constitution"). The United Nations has also established international principles to safeguard such rights, reinforcing their universality.

Data protection, therefore, plays a crucial role in ensuring individual autonomy and in providing a foundation upon which other rights depend. Unauthorised access to personal data—such as financial or health information—can lead to identity theft, discrimination, loss of trust, and other harms that threaten dignity and freedom. This essay examines the relationship between data
protection and other human rights in Nigeria, highlighting recent regulatory developments that have further established this relationship.

Data Protection and the Right to Privacy

Before the enactment of the Nigeria Data Protection Act 2023 (NDP Act 2023), data protection issues in Nigeria were primarily addressed under section 37 of the Nigerian Constitution, which guarantees "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications".

While some commentators have argued that this provision protects only bodily, territorial, and communications privacy, its scope clearly overlaps with data protection. The ability to control the use of one's personal data (data protection) is a natural extension of the right to privacy.

Nigeria's first formal data protection instrument—the Nigeria Data Protection Regulation 2019 (NDPR 2019) issued by the National Information Technology Development Agency (NITDA) marked a significant milestone. However, it lacked the legislative authority and institutional independence necessary for robust enforcement. This gap was filled by the NDP Act 2023, which established the Nigeria Data Protection Commission (NDPC) as the principal regulator for data protection and privacy. Regardless of the limitations, some enforcement actions were issued under the NDPR regime. NITDA sanctioned an online lending platform, Soko Loans, for the sum of ten million Naira (N10,000,000) for revealing customers' phone contacts to third parties. Also, as early as 1967, Alan Westin (a professor of public law and privacy) emphasised that "privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".

The NDP Act 2023 provides a comprehensive framework for protecting personal data and expressly links its objectives to the safeguarding of "fundamental rights and freedoms of data subjects". It applies to all data controllers and processors established in Nigeria or processing data of Nigerian residents, and it mandates the fair, lawful, and transparent processing of such data. By embedding privacy and data protection within a statutory human-rights context, the Act aligns Nigeria's regulatory architecture with global best practices and underscores the constitutional value of privacy.

Data Protection and Freedom from Discrimination

Section 42 of the Constitution prohibits discrimination based on community, ethnic group, place of origin, sex, religion, political opinion, or circumstances of birth. The NDP Act 2023 complements this by requiring that data processing be fair and transparent, with heightened safeguards for "sensitive personal data"—such as information about a person's health, ethnicity, or religion.

Protecting such information is essential to preventing discrimination and social stigmatisation. For instance, unauthorised access to health or religious data can expose individuals to prejudice in employment, education, or other social contexts. Despite constitutional guarantees, discriminatory practices persist in Nigeria, particularly in recruitment and admissions processes. Stronger data protection mechanisms, therefore, reinforce equality by limiting access to information that could be used unfairly.

In this sense, the right to data protection strengthens the right to non-discrimination by ensuring that personal information—which could serve as a basis for bias—remains within the individual's control.

Data Protection, Freedom of Expression, and Association

Section 39 of the Constitution guarantees the right to freedom of expression, including the freedom to hold opinions and to receive and impart ideas and information without interference. Section 39(3)(a) further supports laws that protect confidential information. Inherent in these provisions is the right to data protection—the assurance that private communications will not be unlawfully intercepted or exposed.

The digital environment has expanded the exercise of free expression, particularly through social media. Yet it has also increased vulnerability to privacy breaches. During the #EndSARS protests in 2020, for instance, reports of unlawful access to protesters' digital communications and location data underscored how inadequate data safeguards can chill free speech and deter civic participation.

By protecting personal data and online identities, the NDP Act reinforces freedom of expression and association. Its provisions on security safeguards, breach notification, and lawful processing promote a safe digital environment in which citizens can exercise these rights without fear of surveillance or reprisal.

Data Protection, Human Dignity, and Personal Liberty

Section 34 of the Constitution provides that every person is entitled to respect for the dignity of their person. The European Data Protection Supervisor has observed that "…privacy is an integral part of human dignity and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large-scale personal data processing". In Nigeria, the protection of personal data and privacy thus directly upholds the dignity of individuals by preserving their autonomy and integrity.

Section 35 of the Constitution guarantees the right to personal liberty, which is closely connected to informational autonomy. Individuals should have control over how their personal data is collected, used, and shared. Section 3(1) of the NDP Act reflects this principle by recognising data subject rights such as access, rectification, erasure, and objection to processing. As Frederike Kaltheuner observes, "privacy is fundamentally about human dignity and autonomy." The NDP Act operationalises this philosophy by giving individuals meaningful control over their data and legal remedies when their rights are violated.

Data as Property and the Right to Ownership

Section 44 of the Constitution protects the right to acquire and own property. Although personal data is not explicitly categorised as property in Nigerian law, it shares key attributes of ownership — control, exclusivity, and the right to determine use. Jurisdictions such as the United States treat certain forms of personal data as proprietary interests, allowing individuals to assert rights over its use and enjoyment. In Nigeria, while the NDP Act stops short of this, it grants data subjects enforceable rights akin to ownership, reinforcing the notion that personal data belongs fundamentally to the individual.

Recent Regulatory Developments and Enforcement Trends

Since the enactment of the NDP Act 2023, Nigeria's data-protection landscape has matured considerably. The NDPC has issued the NDP Act General Application and Implementation Directive (GAID) to guide compliance, including the registration of "Data Controllers and Processors of Major Importance" (DCPMIs) and the conduct of Data Protection Impact Assessments (DPIAs) for high-risk processing activities.

In August 2025, the NDPC initiated investigations into organisations suspected of violating the NDP Act 2023, signalling a more assertive enforcement posture. The Commission has also collaborated with sectoral regulators and international partners to promote compliance and cross-border cooperation. Nigeria's cross-border data-transfer framework, now guided by the NDP Act, requires that transfers occur only to jurisdictions ensuring adequate protection or under approved safeguards.

These developments mark a transition from a largely aspirational privacy regime to an enforceable, rights-based data-protection system. They also align Nigeria's framework with global standards and international best practice, while maintaining contextual sensitivity to national priorities.

Conclusion

Data protection and human rights in Nigeria are intrinsically linked, as the protection of personal data underpins the effective enjoyment of other fundamental rights guaranteed by the Constitution. In the digital age, where personal information is constantly collected, used, and shared, data protection safeguards individuals' autonomy, dignity, and freedom from arbitrary interference.

The enactment of the Nigeria Data Protection Act 2023 (NDP Act) has significantly strengthened this relationship by providing a clear legal framework that elevates data protection from a regulatory concern to a right with constitutional dimensions. The Act not only consolidates the principles earlier set out under the Nigeria Data Protection Regulation 2019 (NDPR) but also aligns Nigeria with global data governance standards, ensuring that data subjects can effectively exercise their rights and seek redress for violations.

Importantly, the ruling of the Court of Appeal in Digital Rights Lawyers Initiative v National Identity Management Commission (NIMC) marks a watershed moment in Nigeria's jurisprudence. The court's recognition that the right to privacy under section 37 of the 1999 Constitution (as amended) extends to the protection of personal data resolves years of doctrinal uncertainty. This decision reinforces that data protection is not merely a statutory or regulatory obligation, but a fundamental human right that is enforceable before Nigerian courts.

In essence, data protection is not only a matter of compliance but a cornerstone of democracy and human dignity. It gives meaning to the constitutional guarantees of privacy, liberty, equality, and freedom of expression. The recognition of data protection as a fundamental right provides a constitutional foundation for safeguarding individuals in Nigeria's growing digital economy. Going forward, both state and private actors must integrate human rights considerations into their data processing activities to ensure that technological advancements do not come at the expense of individual rights and freedoms.

THE RELATIONSHIP BETWEEN DATA PROTECTION AND OTHER HUMAN RIGHTS IN NIGERIA

BY

SHINA VICTOR AKINMUSIRE

"Phone Numbers of 9 Million Nigerians Exposed in Latest Facebook Data Breach, NITDA Fines Fintech Firm N5 Million for Data Breach, NITDA imposes N10m fine on firm for privacy invasion", these headlines mirror, in great detail, the current data privacy regime in Nigeria which reaffirms that the discourse on the relationship between data protection and other human rights remains a matter of rapt national concern. Data protection refers to the process of safeguarding personal data from corruption, compromise or loss. The Nigerian digital space witnessed an upsurge of internet users from 85.26 million users in 2020 to 104.4 million users in January 2021. These facts fortify the assertion that data is the pollution of the information age, and protecting privacy is the environmental challenge.

This piece is laser-focused on examining the interrelation between data protection and other human rights as the appreciation of this relationship could be the missing key to the enforcement of data protection in Nigeria.

DATA PROTECTION AND OTHER HUMAN RIGHTS: CONNECTING THE DOTS

In subsequent paragraphs, this essay appraises the interconnection between data protection and the right to privacy, right to information and right to non-discrimination within the scope of the laws on data protection in Nigeria. The unveiling of this interconnection, if any, helps to understand how the breach of data privacy can consequently occasion the infringement of any of the aforementioned rights.

Data Privacy and Right to Privacy: Any Link?

Section 37 of the Constitution of the Federal Republic of Nigeria 1999 as amended guarantees the privacy of citizens, their homes, correspondences, telephone conversations and telegraphic communications. The question as to whether this right extends to the concept of data protection remains lingering in the minds of data subjects and practitioners in Nigeria. This question remains unsettled.

A school of thought holds that it is disingenuous to take data protection and privacy as the same, and thus, a misnomer to categorize it as a fundamental human right. It opines that right to privacy exclusively deals with the privacy of Nigerian citizens while data privacy is a universal concept and it cannot be restricted to a particular geographical area. Furthermore, it posits that the right to privacy is limited to their homes, correspondences, telephone conversations and telegraphic communications and does not include the definition of personal data as stated in Section 1.1 of the Nigeria Data Protection Regulation (NDPR). Contrastingly, another school of thought contends that data protection has a strong attachment with the right to privacy as well as other human rights which arguably makes it a human right too.

Unfortunately, the Nigerian courts have, by conflicting decisions, compounded the confusion on the relationship between data protection and the right to privacy. The Federal High court in Digital Rights Lawyers Initiative v. Unity Bank held that data protection has nothing to do with the right to privacy and actions bordering on data breach cannot be validly brought under fundamental rights procedure. By contrast, the Ogun State High court in Digital Rights Lawyers Initiative v. National Identity Management Commission categorically held that the right to privacy extends to data protection. The position as to whether data privacy is subsumed under the right to privacy remains unsettled until the appellate court pronounces on this very fundamental issue.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

In international jurisprudence, it is well-established that data protection is subsumed under the right to privacy. This position can be gleaned from Article 8 of the Charter of Fundamental Rights of the European Union which provides that "everyone has the right to the protection of personal data concerning him or her". Additionally, the 2012 Association of Southeast Asian Nations (ASEAN) Human Rights Declaration marries data protection and data privacy by including personal data in the items protected under the right to privacy.

This piece supports the classification of data protection as a human right originating from the right to privacy. This is because all human rights are universal, indivisible, interdependent and interrelated. Additionally, the Fundamental Human Rights Enforcement Procedure Rules, 2009 empowers the court to expansively interpret and apply the rights and freedoms contained in 1999 Constitution with a view to advancing and realising the intended protections. By this approach, right to privacy should be expansively interpreted to cover data protection.

Data Protection and Right to Information: Any Connection?

The right to information is a right derived from the freedom of expression which ensures access to information held by government bodies. By this right, a public body is legally obligated to provide certain information to a person requesting for such information except where a legally compelling reason to decline the request exists. In Nigeria, the Freedom of Information Act is the statutory framework enacted to protect this right as Section 39 of the 1999 Constitution merely mentions it.

The relationship between data protection and right to information is symbiotic. They are complementary. The common purpose of these rights is to ensure the secrecy of citizens' personal information in an information-crystallized society while maintaining the transparency and accountability of the government.

While data protection and right to information might complement each other, there might be conflicts especially where the government improperly cites data protection as an excuse to revealing certain information. This piece recommends that this conflict can be resolved by the establishment of oversight systems and entrenchment of clear definitions in data protection legislations.

Data Protection and Right to Non-discrimination: Any Nexus?

The right to non-discrimination is protected under Section 42 of the 1999 Constitution. The interconnection between this right and data protection is the effort towards ensuring an individual's control of information which could cause discrimination if known to a third party. The relationship between the right to non-discrimination and data protection exists in situations where the leak of a person's information or characteristics may result in discrimination. Practically, the ability to jealously guard information bothering on religion, health status, gender identity or sexual orientation ensures protection from discrimination. Simply put, unauthorized access to an individual's personal data may conjunctively constitute a breach of data privacy and the right to non-discrimination.

Furthermore, discrimination may also occur during the processing of personal data. This is referred to as profiling. Profiling can be used by the government and private institutions to reach decisions which determine what sort of treatment a person gets and what services they enjoy. By profiling, a person is put at the risk of facing discrimination due to a particular unfavourable characteristic they possess. To eliminate this possibility, the Section 6.2 of the Implementation Framework of the NDPR protects the processing of personal data such as ethnic or political affiliation, religious belief, and sexual orientation amongst others. In 2016, the European Union enacted the General Data Protection Regulation (GDPR) which mitigates this particular risk as it affords data subjects the right against a decision based solely on automated processing such as profiling.

CONCLUSION

Understandably, data protection in Nigeria is still in its salad days, and no doubt in dire need of the consolidated action of the public and private sectors to address the existing inadequacies of the laws guiding data protection. Having established the relationship between data protection and other human rights, it is concluded that it is symbiotic. Consequently, the breach of data privacy can as well lead to the breach of other human rights and this lends credence to why data protection should be recognized as a human right. Importantly, the Nigerian judiciary must rise to its judicial task by providing authoritative resolutions to the status of data protection.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

THE RELATIONSHIP BETWEEN DATA PROTECTION AND OTHER HUMAN RIGHTS IN NIGERIA

BY

DUREKE CLINTON CHARLES

1.0. INTRODUCTION

As aptly noted by the United Nations Office of the High Commissioner for Human Rights, all human rights are indivisible and interdependent. A set of rights cannot be enjoyed fully without the other. There is thus a limit to which a human right can advance without other human rights being guaranteed and enforced. Accordingly, the right to privacy and data protection interplays with other civil and political rights guaranteed under Chapter IV of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) ("the Constitution"). Data protection has been settled to come within the ambit of Section 37 of the Constitution, by a ruling of the Court of Appeal in the case of Digital Rights Lawyers Initiative v National Identity Management Commission. The section guarantees the protection of the privacy of Nigerian citizens, their homes, correspondence, telephone conversations and telegraphic communications.

This essay will examine the interplay between the right to privacy and data protection and three rights in particular: the right to personal liberty, the right to freedom of expression and the press, as well as the right to freedom of peaceful assembly and association. Coupled with Chapter IV of the Constitution, recourse will also be made to the relevant provisions of the African Charter on Human and Peoples' Rights ("the Charter"). The ratification and enforcement of the latter was upheld in the case of Abacha v Fawehinmi.

2.0. THE RIGHT TO DATA PROTECTION AND THE RIGHT TO PERSONAL LIBERTY

Section 35(1) of the Constitution provides inter alia that every person shall be entitled to his personal liberty and no person shall be deprived of such liberty. This is subject to specified qualifications, which must accord with a procedure permitted by law. In the same respect, Article 6 of the Charter provides inter alia that every individual shall have the right to liberty and to the security of his person and that no one may be arbitrarily arrested or detained.

In the Nigerian context, a strong correlation can be identified between the right to privacy and data protection and the right to personal liberty. While Section 29 of the Police Act 2020 mandates police officers to detain and search persons upon reasonable suspicion and prima facie hints at an objective standard in stop and search contexts, members of the Nigerian Police Force are notorious for simultaneously infringing on the personal liberty and data privacy of citizens based on frivolous grounds. Electronic devices like smartphones and laptops are typically seized by Nigerian Police officers under the guise of criminal investigations, with the police officers going on to access the personal data of victims in an irresponsible manner. In November 2019, a Nigerian man was reported to have been extorted of fifty thousand naira by officers of the infamous Special Anti-Robbery Squad (SARS) for refusing to unlock his phone as demanded by the officers. This state of affairs is worsened by the fact that no clarification is rendered for the term, "reasonable suspicion" in Section 1 of the Police Act 2020, the interpretation section.

In a nutshell, many Nigerians are put in positions where they have to choose between their right to personal liberty and their right to privacy and data protection. More often than not, the latter takes the fall. Concerted efforts are thus required to mitigate the continuous infringement of the right to privacy and data protection by members of the Nigerian Police Force.

3.0 THE RIGHT TO DATA PROTECTION AND THE RIGHT TO FREEDOM OF EXPRESSION

Section 39(1) of the Constitution provides that every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference. It is further provided in Section 39(3) that nothing in the section shall invalidate any law that is reasonably justifiable in a democratic society for the purpose of disclosure of information received in confidence, maintaining the authority and independence of courts or regulating telephony, wireless broadcasting, television or the exhibition of cinematograph films.

A subset of the right to freedom of expression which pertains more to journalists can be deduced from Section 39(3), being the right to not be compelled to disclose confidential information. In addition, the phrase, "information received in confidence" can be read in conjunction with the phrase, "correspondence, telephone conversations and telegraphic communications", given that sensitive information is typically shared via the latter media.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Furthermore, in line with the primary duties of the press such as news reporting and the aggregation of public opinion, print and media establishments may be regarded as Data Controllers. Section 65 of the Nigeria Data Protection Act, 2023 ("NDPA 2023") defines a Data Controller as an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data. Essentially, print and media establishments have an obligation to properly process and safeguard the numerous data from which news is distilled.

While a link can be clearly identified between the right to freedom of expression and the right to privacy, the latter specifically relating to data protection and privacy, it is submitted that the government ought to do more in the area of policy making. There is enough room for proposed policies which factor in both fundamental human rights, coupled with the need to enlighten the citizenry and make media establishments more conscious of the implications of their decisions.

4.0. THE RIGHT TO DATA PROTECTION AND THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

Section 40 of the Constitution provides inter alia that every person shall be entitled to assemble freely and associate with other persons. Similarly, Article 11 of the Charter is of the effect that every individual shall have the right to assemble freely with others, subject only to legal restrictions in the interest of national security and the safety, health, ethics, rights and freedoms of others.

In recent times, the issue of privacy and data protection has emerged on the front burner of the right to peaceful assembly and association. While the substance of Section 40 of the Constitution may easily be construed strictly in the physical sense, online assemblies have gained traction in recent times. The #EndSARS protests in Nigeria, a recurring decimal in the Nigerian public discourse which culminated in nationwide protests in October 2020, perfectly encapsulate the modern significance of online assemblies. However, recent advancements in biometrics-based facial recognition technology and the interception of communications have eased the task of State actors in surveilling protests. The growth of targeted surveillance against activists and civil society organisations has also been observed, coupled with the lack of transparency on technology use, technology access and how data collection is handled.

The foregoing developments pose a dual risk to the right of citizens to freely assemble without apprehension and to not have their sensitive data compromised in a life-threatening way. Public confidence in this regard has also been dampened by the directive given by the Nigerian Communications Commission (NCC), mandating Mobile Network Operators to update their SIM registration records with the National Identification Numbers of all their subscribers. While the directive could have been met with less cynicism in a different context, it was issued barely two months after the #EndSARS protests of October 2020.

5.0. CONCLUSION

While it may not meet the eye upon first glace, the right to data privacy and protection is intricately tied to a handful of the civil and political rights recognised by the Constitution. In theory, redress for the infringement of any of the highlighted rights pursuant to Section 46 of the Constitution can also incorporate the enforcement of one's right to data protection. Thankfully, plaintiffs in this now have more relevant precedents to rely upon due to increasing awareness of data privacy rights and judicial activism in this regard. To supplement Nigeria's growing legal framework on data protection, it is recommended that the federal government should make concerted efforts towards the formulation and implementation of policies geared towards reinforcing data protection as a key facet of other human rights in Nigeria.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

INCREASING PRIVACY REGULATION: A CATALYST OR BARRIER TO TECHNOLOGY INNOVATION

BY

GABRIEL OMONIYI

Introduction

Prior to Edward Snowden's revelation in 2013 about the connivance of the United States of America's National Security Agency, the Federal Bureau of Investigation, the United Kingdom's General Communications Headquarters and nine giant tech companies on its collection of data from these companies; the discussion of privacy in Europe has never been a front-burner issue. In fact, the first major policy attempt at privacy regulation in Europe only came to the fore in 1995 following the issuance of the 1995 Data Protection Directive (Directive) by the European Council. Thereafter, the General Data Protection Regulation (GDPR) which is broader than the GDPR and provides for more rights, obligations and liabilities was adopted by the European Union in 2016 and became applicable across all European countries. Coming home to Nigeria, Nigeria though late to the party issued her first data privacy and protection specific provisions in 2019 – the Nigerian Data Protection Regulation 2019 (NDPR), and the NDPR Implementation Framework in November 2020; and began to enforce some of its provisions. With these legislations on the global scene and particularly in Nigeria, there has been an increase in the awareness and concern of privacy especially for individuals.

More recently, there has been a discussion about implementing data localisation (DL), a term which refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a jurisdiction. Flowing from all these, the question is whether furthering privacy regulation (PR) can stifle technology innovation. Simply defined, PR is any form of enactment or measures put in place by regulatory authorities or legislation to ensure the security of data of any data subjects in the care of another person. While this may be multi-twisted, it is never in doubt that a further enactment and enforcement of privacy will have both positive and negative impacts on technological innovations in Nigeria and the world at large.

Privacy Regulation from a Technological Perspective

The concept of privacy, which has had a long history as far as the period of colonialism of America, and developed all through to international instruments like the Universal Declaration of Human Rights 1948 (art 12), does not address the present-day realities of data collection, privacy, and processing, hence, a need to enact legislative provisions such that will fill this vacuum. Prior to the NDPR, the right to privacy under section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) - which was the major provision on privacy - only extended to informational privacy, and does not impose some specific rights and obligations on the data subjects (DS), data controllers (DC) and/or data processors (DP). It is based on these that statutory cum regulatory instruments like the NDPR in Nigeria, GDPR in Europe and the California Consumer Privacy Act, 2018 in the State of California were enacted to cater for the DS and regulate the operation of the DC and the DP.

Boosting Innovation through Privacy Regulation

One of the major benefits of an increased PR is the increased trust by the DS. Considering the present day relevance of data gathering, an increased trust will lead the DS to often give accurate data to the DC, and which in return lead to improved innovation. According to a survey conducted by Deloitte, two-thirds of consumers believe retailers use their data for targeted marketing, while more than half think retailers share data with third parties or sell it to outside buyers and thereby may be reluctant to further give their data out. The result of this lack of trust will therefore lead to the DS being drawn aback to either giving complete or accurate information to the DC. Thus, improving the PR will in return better the lots of innovation through accurate and complete data gathering.

Another benefit of an increased PR is the technological advancement it will result in. For instance, the full implementation of DL in Nigeria will lead DC to implement data safety innovations within the country that ordinarily would have been outsourced to foreign firms.

By so doing, there is technological advancement, investment in capital projects that guarantee and sustains data privacy and capacity building for Nigerian employees.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

In addition, an increased PR can incentivise innovation on a grand scale. As noted by the International Association of Privacy Professionals (IAPP), the number of the privacy technology vendor market which stood at 44 in 2017 has now within a 5-year bracket reached 355 in 2021. The import of this is that there will be an upward trend in technological researches and advancements to simplify data collection and processing. Borrowing an analogy from the Financial-Technology sector in Nigeria, an increased regulation from the relevant authorities have furthered the amount of investment, trust and improvement in offering financial services to the public.

Increased Privacy Regulation as Barrier to Technology Innovation

Notwithstanding the above-mentioned benefits of increased PR, there can be an increased cost of compliance on the part of the players in the data industry. As it stands in Nigeria, all DC are expected to have a well-detailed privacy policy, make periodic filings with NITDA and engage the service of a Data Protection Compliance Organisation (DPCO) who will conduct impact assessment and audit at regular intervals, amongst other requirements. Thus, increasing compliance burdens on businesses in Nigeria will not only redirect the focus of such firms from innovation to compliance but also increase their risk and expenditure on compliance-related costs, thereby impacting their bottom line.

Another effect of PR is its effect on innovation globally. Maintaining a strict compliance stand on DL as an example will often result in an increased cost of local employment and infrastructure investment, result in efficiency losses such as disruptions to global consolidation plans and skill dilution, and increased compliance costs and uncertainty from meeting many localisation requirements. The impact of this will eventually be transferred and borne by the DS who as the final consumers will pay for these increases and impact.

An increased PR may be counter-productive in a free market economy. As discussed above, with the increased cost that comes with an increased PR, bigger firms considering their deep pocket may find it seamless to comply with many of these laws thereby leaving out small and medium-sized enterprises (SMEs) to struggle with these obligations under these regulations. This will no doubt affect the plight of many business, most especially in Nigeria where the SMEs contribute about 50% to the nation's Gross Domestic Product. As rightly noted by some commentators, 'privacy protection may stifle innovation outside the structures developed by a handful of leading players.'

Conclusion

As analysed above, increasing PR is a dicey situation that has two sets of distinct impacts on every country. Thus, in harnessing the benefits that come from PR, the cost-benefit and economic implication of a full-blown increased PR must equally be considered. While it is agreed that technology has become a daily necessity and an encroaching concept to the minutest part of life, sensitization of the populace can be a tool to combat some of these privacy-impacting innovations. Regulatory bodies, most especially in Nigeria, must while striving to make the polity an investment destination, be proactive in protecting her citizenry and calling out infringing applications and companies for violations of the privacy of her citizens and avoid pushing off enterprises that could have bettered the lot of businesses and individuals in Nigeria. In the words of Ramanchandran, 'innovation and privacy are compatible — innovation cannot be scaled without adequate privacy safeguards and gaining users' trust. It is critical to empower users, without over-regulating data collection.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

INCREASING PRIVACY REGULATION: A CATALYST OR BARRIER TO TECHNOLOGY INNOVATION

BY

CHIDERA EMMANUEL CHIKERE

Background

Increasing technological advancement is continually changing the narratives and scope of corporate assets. Traditionally and since the industrial revolution, business assets have always been characterised in terms of property, plants, equipment, inventories, and human resources. However, with optimised digital infrastructure, businesses, organisations, and even governments continue to adapt to take advantage of the boundless opportunities which technology offers, such as artificial intelligence, deep learning and big data analysis. Consequently, this has led to the new revolution, the dawn of the era marked by an overwhelming reliance on data. IBM defines big data as data sets whose size or type is beyond the ability of traditional relational databases to capture, manage and process the data with low latency.

Personal data is generated on a large scale every day; when we open a mobile app, search a restaurant on Google, post a picture on the social media, shop online, make payments, or simply use GPS to travel from one place to another. Technologies, such as 5 G-enabled sensors, face and voice recognition, are now deployed across different platforms, generating invaluable set of personal data. With systems such as artificial intelligence, deep machine learning and analytics, even the tiniest, the most unstructured and most superficially unintelligible data is now the new oil. Companies regularly capture, store, and analyse large amounts of quantitative and qualitative data on their consumer base every day, from consumer behaviour to predictive analytics, to drive knowledge and value creation across societies, fostering new products, processes, markets, and business models.

Admittedly, the collection and analysis of data have helped businesses to improve decision-making and their offerings by creating personalised services tailored to the preferences of their consumers and thereby enhancing economic competitiveness and productivity growth.

On the flip side, personal data has also become susceptible to mismanagement and abuse by data controllers and managers. Unethical dealings resulting in high-profile data breaches and privacy infractions, such as the Cambridge Analytica scandal, where over 87 million individuals had data illegally mined on some of the world's largest social media outlets, have made many consumers increasingly sensitive to how their data is used and protected. It is on the backdrop of these susceptibilities and pitfalls that privacy regulations are increasingly being rolled out and business as well as public institutions are required to comply with their operations. With regulations in the mix of the train of data-driven advances, the question is, are privacy regulations a catalyst or barrier to technology innovation?

This article analyses the impact of privacy regulation on innovation and takes the position that data-driven innovation is a product of increased and improved privacy regulations. it further identifies this catalyst in terms of a corresponding responsibility and transparency by data administrators, managers and controllers, which will engender consumer trust and confidence in the digital economy and improve the truth value of the data needed for innovation.

Privacy Regulations and Innovations

Innovation is the implementation of a new, significantly improved product (goods or service) or process. It is the introduction of a good or service that is significantly improved with respect to its characteristics or intended uses, extending to significant improvement in technical specifications, components and materials, incorporated software, user-friendliness and other functional characteristics. In relation to process or procedure, innovation is the implementation of a new or significantly improved production or delivery method or delivery method. It is difficult to separate a discourse on data-driven technology innovation without an interface with privacy regulations. Regulations are any general form of coercive or directional rule-setting by policymakers to influence market activity and economic actors' behaviour. In particular terms, privacy regulations are rules specifying the legal latitude in which data can be processed.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Across jurisdictions, a network of privacy laws and data protection frameworks has emerged to govern the collection and use of personal data. The European Union's General Data Protection Regulation (GDPR) was the global benchmark which influenced the design of data protection regimes in several jurisdictions, including Nigeria. In Nigeria, the Constitution of the Federal Republic of Nigeria (1999) (as amended) recognises the right to privacy under Section 37, while the Nigeria Data Protection Act 2023 (NDPA) establishes the comprehensive framework for personal data processing, extending and formalising the earlier Nigeria Data Protection Regulation 2019 (NDPR).

The unifying principle across these instruments is the establishment of lawful bases for data processing built on consent, transparency, and accountability, placing an affirmative duty on data controllers and processors to prevent unauthorised disclosure, misuse, or cross-border transfer of personal data.

Given the central role of personal data in contemporary business and financial models, entities whose activities fall within the scope of these regulations ordinarily perceive them as constraints on commercial discretion, since they limit what firms can legally collect, analyse, and monetise. By limiting what firms can legally do with personal data, privacy regulations appear to impose compliance costs that could potentially stifle innovation. However, when we look beyond regulations and towards opportunity, we see that these frameworks creates a trigonometric chain of positive impact across the economic value chain.

First, privacy regulations impose higher standards of responsibility on data controllers and managers, driving the development of sophisticated governance systems and compliance technologies. Second, they empower data subjects through consent and access rights, strengthening their control over personal information. Third, these mechanisms enhance consumer trust and confidence in digital transactions, a factor that directly influences financial inclusion and market participation.

Responsibility, Accountability and Transparency

The immediate impact of the diverse and expanding privacy regulations is responsibility, the obligation on data controllers and processors to comply with the law, confer the benefits envisaged by the rules, and refrain from acts prohibited by them. Article 5(1) of the GDPR provides that personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject. This principle is also provided for in Section 24(1) of the Nigeria Data Protection Act, 2023 (NDPA), which requires that personal data be processed in a lawful, fair, and transparent manner. Transparency is exhibited through three interrelated elements: notice, choice, and access.

By way of notice, data controllers are mandated to provide privacy policies in clear and easily comprehensible language, informing the data subject of the nature and purpose of data processing. Section 27(1) of the NDPA reinforces this obligation by requiring data controllers to provide data subjects with detailed information about the categories of data collected, the lawful basis for processing, the recipients of such data, and the rights available to them.

The principle of choice empowers the data subject to determine whether their personal data may be processed, consistent with Section 26(1)(a) of the NDPA, which establishes consent as a lawful basis for processing. The data subject retains the right to withdraw such consent at any time and to request the deletion of personal data, as recognised under Section 34(1)(e) of the NDPA. The pillars of openness, transparency, and accountability are further sustained by implementation mechanisms such as the appointment of Data Protection Officers (DPOs) under Section 32 of the NDPA ensures institutional compliance and continuous monitoring of data-handling practices. These officers serve as internal custodians of compliance, promoting adherence to lawful processing principles.

These mechanisms shift the balance of power from a corporate-advantaged position to a consumer-oriented perspective, enabling individuals to exercise control over their data, thereby fostering trust and confidence in digital ecosystems.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Consumer Trust and Confidence

The Ultimate goal and end of advances in technology-backed solutions and innovations is public confidence, sustained patronage, and continual use. As a matter of fact, novel technology-backed solutions often encounter initial scepticism and may face conservative distrust. Such soluito at their early stages often face a form of conservative distrust and may take a period of time-test to gain consumer confidence and reenforce acceptability. A principal source of this distrust lies in the collection and use of sensitive personal data required for the operation of these platforms. For instance, a number of financial technology, healthtech, and digital identity systems in Nigeria request sensitive credentials such as the National Identification Number (NIN), Bank Verification Number (BVN), biometric identifiers, and payment authentication details.

Empirical studies show that privacy concerns have a direct impact on consumer trust and alter consumer behaviour in a number of negative ways. According to a study by Deloitte, a majority (73%) of respondents indicated that they are more likely to be open to sharing their data when privacy policies are clear on how the data will be used and if they are confident that protective safeguards are in place. In practical terms, where such confidence is absent, it is not uncommon for such users to supply inaccurate information in an attempt to remain anonymous or entirely abandon transactions midway out of scepticism about data use, particularly in relation to financial details, passcodes, or medical information. The consequence of this trust deficit is that much of the information collected by digital platforms becomes unreliable, increasing operational costs while reducing data quality and economic value.

The cornerstone of trust in the digital economy and governance are security, privacy and consumer protection. Investment in these pillars, particularly through the consistent enforcement of privacy regulations will yield dividends in form of enhanced innovation and sustainable growth. Consumer trust is fostered by confidence in the transaction processes or procedures, and in the rules and protocols that monitor the performance and control of transactions which in fact among many others are privacy regulations.

The upside is that consumers are more likely to continue the use of services in which they can repose their trust and confidence. If it data drives innovation; then its reliability is inseparable from the truth value of the data collected. Privacy regulation, therefore, enhances both the accuracy and availability of data, thereby fostering confidence in emerging technologies and driving demand for new, data-driven solutions.

Conclusion

Data remains the fuel on which many innovations thrive, from artificial intelligence systems that optimise decision-making to predictive analytics that power modern governance and commerce. To assess the impact of increasing privacy regulation on technological innovation, it is essential to take time frame into consideration and look beyond the short term. Disruptive effects may predominate initially, as new regulations unsettle existing models of data. However, in the medium to long term, the effects of privacy regulation are positive and sustainable.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

INCREASING PRIVACY REGULATION: A CATALYST OR BARRIER TO TECHNOLOGY INNOVATION

BY

OLAWOYIN MUSTAPHA TOLANI

1.0 INTRODUCTION

"The world's most valuable resource is no longer oil but data"

The importance of data in today's world cannot be overemphasised. It is the major driver of the digital economy. The unprecedented development in technology innovations has upped the need for data. Practically, most of these tech inventions only operate efficiently with data. This therefore underscores the need for data regulations to prevent the misuse, abuse and misappropriation of personal data of users. For instance, in 2015, the private data of more than 80 million Americans were harvested on Facebook by Cambridge Analytica, a data mining firm, to influence the 2016 United States Presidential Election in favour of certain politicians. An investigation carried out in 2018 showed that Facebook mishandled the data, making it accessible to Cambridge Analytica. Similarly, top tech giants like Google, Alibaba, Amazon have been accused of such breach. However, the ongoing debates in the data privacy space is on whether technological inventions will be affected by the rise in privacy regulations. This writer believes that, even with some protective benefits, the increasing regulations on privacy are now becoming a barrier for efficient technological innovations. This essay is structured into different parts. A part will examine the key terms, while another part will look at how privacy regulations are increasing around the world. The final part will look at how these regulations stifle technological innovation both around the world and specifically in Nigeria.

2.0. DEFINITION OF KEY TERMS

2.1. PRIVACY -according to Merriem Webster dictionary, it is the freedom from unauthorized intrusion. In this context, it is the protection of the personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information. Specifically in Nigeria, the concept of privacy can be hinged on the Constitution of the Federal Republic of Nigeria, particularly Section 37.

This provision ensures the right of every citizen of Nigeria against intrusion of privacy by other persons without consent. An extension of this right is Privacy as it relates to personal data/ information collected by groups, businesses, organisations, and even government parastatals known as "Data Controllers".

2.2. TECHNOLOGICAL INNOVATION- A technological innovation is a new or improved product or process whose technological characteristics are significantly different from before. Implemented technological product innovations are new products (product innovations) or processes in application (process innovations) that have been brought to market. It is also said to be the commercialization of a technical idea through productive design, development and implementation of a technology-based product, service or a process making significant technological changes to address customer needs, wants or a problem in the market.

3.0. INCREASING PRIVACY REGULATIONS AROUND THE WORLD

Like never before, there has been an increase in privacy regulations around the world. This is because of the exponential growth in the number of data being shared over the internet with organizations and businesses online by internet users. Therefore, countries are coming up with different enactments to regulate and protect this data. As at 2021, of the 195 countries in the world, 128, representing 66%, have enacted legislations and regulations on data protection and privacy. Prominent among these regulations is the General Data Protection Regulation (GDPR) which was passed in 2018. The regulation applies to any organization that collects and processes the data of any European Union citizen. In a similar style, the California Consumer Privacy Act (CCPA) was passed in 2018. The legislation gives data subjects the right to know how and what their data is being used. Brazil recently passed its general data protection law called the "Lei Geral de Protecao de Dados Pessoais" effective 2020 which made an outline of data processing standards in the country. In 2017, Argentina passed the National Directorate of Personal Data Protection to replace the Personal Data Protection Law 2000. In South Africa, the Protection of Personal Information Act 2014 regulates data protection in the country.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

In Canada, the "Bill C-11, the Consumer Privacy Protection Act (CPPA)" was introduced on November 17th, 2020 to amend the Personal Information Protection and Electronic Documents Act (PIPEDA). In Singapore, the Personal data Protection Act, effective February 2021 regulates data privacy and protection in the country. Others are Thailand's Personal Data Protection Act, 2019;

The trend is not any different in Nigeria. Although the country does not have a comprehensive legal framework for data protection and privacy, there are, however, sectoral regulations addressing some privacy issues. More so, in 2019, the National Information Technology Development Agency issued the Nigeria Data Protection Regulation which now serves as the principal legal framework on data privacy in Nigeria. The regulation applies to all natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria. Apart from the NDPR, there are sectoral regulations with provisions relating to data privacy. For instance, the Central Bank of Nigeria issued a Consumer Protection Framework to all financial institutions in the country which contains provision on the protection of the customers data.

Against the above backdrop it is evident that regulations on data privacy and protection keep popping daily from countries around the world. A number of countries without an extant regulation are also making plans to promulgate one in the foreseeable future.

4.0. INCREASING REGULATION ON PRIVACY AS A BARRIER ON TECHNOLOGICAL INNOVATION

It is undeniable that having regulations on data privacy ensures the protection of people's right to privacy. It prevents the sharing of a person's information without express consent or using the information obtained for a purpose totally different from what it was originally intended for. However, the growing rate of regulations from different sectors and agencies which data-driven tech companies have to comply with is tedious. These regulations are now in the process of stifling technological innovations. Compliance with these unending privacy laws and regulations comes with higher costs on the part of the companies. Revenue which originally should have been used for innovating new products are instead deployed to privacy compliance officers and filing different privacy compliance reports with different agencies.

For instance, going by a PwC report in 2017, more than 40 percent of firms who responded to a survey carried out by PwC spent over $10 million on GDPR compliance efforts. Similarly, according to a joint report by the International Association of Privacy Professionals in 2018 concluded that companies reported spending an average of $1.3 million per year on GDPR compliance cost alone. In a survey carried out by Reuters, it was observed that companies in the United Kingdom reported that the largest portion of budgets goes to GDPR at 43%. Also, privacy related expenses have reportedly increased in Canada, Australia, New Zealand and France.

Privacy regulations, particularly the GDPR, require data controllers to create the office of Data Protection Officer ("DPO"). According to recent study by the International Association of Privacy Professionals (IAPP), estimates that as much as 75,000 Data Protection Officer jobs will be created in response to the GDPR around the world. This also comes at a cost to the company or organization because the DPO will be remunerated for his work either as an employee or a freelance professional. This shows the outrageous costs that start-ups need no bear so as to certify their compliance to privacy regulations. In a similar breath, Adam Thierer & Ryan Hagemann suggest that regulations on the collection and use of personal data in the field of driverless vehicles, for instance, will lead to higher costs for start-ups and small operators, and prevent consumers from enjoying the potential benefits of innovation.

Therefore, if revenue is affected by the high cost of compliance, investment opportunities especially from venture capitalists may be affected. Companies may therefore switch their business model by making some of their services (which were originally free) premium based, all in a bid to bridge the costs spent on regulatory compliance.

Another stifling effect of the increasing regulations on privacy is that they limit the use of data for research purposes. Without these researches, the world may never benefit from the possibilities of some technological innovations and emerging technologies. For instance, Artificial Intelligence and Internet of Things are some of the emerging technologies shaping the world.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

However, these technologies need to be effectively trained with sufficient data for them to function efficiently. A greater importance of data for research became obvious during the peak of Covid-19 pandemic. Data from around the world helped medical practitioners and healthcare professionals in the fight against the virus and ultimately came up with vaccines. Also, the United States and other countries deployed GPS trackers to monitor the location of people who are believed have been exposed to the virus. This would not have been possible if there were a truckload of privacy regulations to comply with.

Some may argue that instead of stifling, these regulations have a spurring effect on innovation. However, this can easily be displaced by the report that shows that there are more technological innovations in the United States which has less privacy regulations than Europe with more stringent and increased regulations.

5.0. NIGERIA AS A CASE STUDY

Technological innovations in Nigeria have been on the rise since the introduction of the internet in the country. A growing number of tech solutions have been and are being developed daily across sectors -finance, health, education, and agriculture, to mention a few. The likes of Remita, Paystack, Flutterwave, Babymigo, Hotelsng, uLesson,Gradely, Thrive Agric, among a long list of others are products of technological innovation in the country.

Like earlier mentioned, most of these innovations thrive on user personal data to make near-accurate predictions using Artificial Intelligence and provide better services to users. However, compliance with the numerous sectoral regulations on privacy still poses a great threat. According to the Director General of the National Information Technology Development Agency, Khashifu Inuwa Abdullahi, only 588 entities in the country complied with the NDPR in 2020. This is because compliance comes with a huge cost on the companies.

6.0. CONCLUSION

Against the above backdrop, it can be observed that this is a tussle between encouraging innovations and individual fundamental right to privacy. Admittedly, privacy regulation is necessary but proliferation of these regulations will only have a stifling effect on technology innovation.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

A LONG WALK TO FREEDOM: NIGERIA'S DATA PROTECTION JOURNEY

BY
OLONI OPEMIPO

Imagine a world where Shoprite knows what you want before you do, where Netflix magically knows the kind of movies and series that you like, where the ads that pop up on your Facebook just happen to meet your preferences or a world where companies like InfiniGraph or Rapleaf make millions of dollars from gathering (mining) and selling personal information of individuals. You don't have to imagine anymore; this is the world we live in. In the digital era, personal information (Data) is the new oil. It is interesting to note that Internet users generate about 2.5 quintillion bytes of data each day, and by 2020, there will be around 40 trillion gigabytes of data (40 zettabytes). This is the world we live in; a world where data is more valuable than gold.

In today's global economy more countries are waking up to the effects of data breaches and the need for organisations to protect customers personal information and as such are enacting effective legislation to deal with this. This need has also been identified by international organisation who have realized the inevitability of cross border transfer of personal data across jurisdictions. Therefore, these organisations have developed conventions, regulations, charters and model bills for the protection of personal data and information. As at June 2018, 126 countries now have data privacy laws which at least meet the ten minimum standards set by international agreements as early as 1980 and 45 of the 126 laws have been enacted in the last decade with an average of 5 new laws per annum.

In Africa, regional bodies have invested efforts in ensuring that data protection and privacy are prioritised by Member States. For instance, in 2014 the African Union (AU) adopted the Convention on Cybersecurity and Personal Data Protection. In 2010, the Southern African Development Community (SADC) developed a model law on data protection which it adopted in 2013. In 2010, the Economic Community of West African States (ECOWAS) adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS. The East African Community, in 2008, developed a Framework for Cyberlaws.

Notwithstanding these efforts, many countries on the continent are still grappling with enacting specific legislation to regulate the collection, control and processing of individuals' data. Nigeria appears to fall in this category. Since 2008, 6 data protection bills have been introduced in the National Assembly. None of these bills have been passed into law. While there is no omnibus data protection legislation, there are various regulations sector specific legislations that have been developed

over the years. They include the Credit Reporting Act 2017, The Cybercrimes Act 2015, etc. landmark among these regulations is the NITDA Guidelines for Data Protection 2019

In January 2019, the National Information Technology Development Agency ("NITDA") acting within its authority to plan, develop and promote the use of information technology in Nigeria, issued guidelines on data protection; the NITDA Data Protection Regulations (NDPR). The NDPR was introduced to raise the Nigerian Data protection standards to meet up with GDPR standards. The NDPR is an improvement upon the Guidelines on Data Protection issued by NITDA in 2013. It is more robust and comprehensive, and it imposes penalties for non-compliance with its provisions. It also grants enforceable rights to data subjects.

The GDPR which represents the highest international standard in Data Protection in the world today was introduced in April 2016 and set to come into force on May 25 2018. The Regulation repealed the Directive 95/46/EC (Data Protection Directive).

The NDPR is a landmark achievement in data protection in Nigeria which is a becoming a largely digitalized economy. The regulation is to a large extent modelled after the GDPR. The NDPR has adopted or replicated some of the key provisions of the GDPR, including Fair Information Principles (FIPs) which are an exact duplicate of the principles enshrined by the GDPR.

Nonetheless, the Regulation is not as comprehensive and extensive as the GDPR. Furthermore, there is a question of if the timeline given for the effectiveness of the Regulation is practicable. The Regulation is set to take effect when it is signed by the NITDA Board; it is to be noted that the Regulation was issued on the 28th of January 2019, and it mandates companies to comply with its provisions from the date of issuance of the Regulation.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

The full implementation of the Regulation commenced on 25th April 2019.This is a remarkable contrast from the GDPR which provided for a two-year period within which member states of the European Union (EU) were to comply with it. Considering that this legislation on data protection is relatively novel in Nigeria, it may take some time for companies and businesses to fully comply with it.

The emergence of a generally applicable data protection regulation in Nigeria is most welcome. However, the regulation is not the long-awaited safety net for personal information, but a mere band-aid. The Regulation is significant to the extent that it fills the longstanding void in the regime for data protection in Nigeria and mitigates the challenges occasioned by this void. Regardless of its inadequacies, the NDPR would without doubt aid in providing some degree of safety to personal information, consequently fostering competitiveness of Nigerian businesses in international trade and boosting the confidence of individuals in digital processes.

On 28 June 2019, in the case of Incorporated Trustees of Paradigm Initiative for Information Technology (PIIT) & Sarah Solomon-Eseh v National Identity Management Commission (NIMC) & Anor the Federal High Court of Nigeria affirmed the data privacy rights of Nigerian citizens and directed the National Identity Management Commission (NIMC) to improve on its data privacy and security systems in order to avoid a breach of citizens' rights to privacy. This decision is a breakthrough for data privacy in Nigeria. However, Nigeria is still a long way from the promised land as a lot still needs to be done to ensure compliance with international standards for data protection.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

PROVIDE AN ANALYSIS OF NIGERIA'S DATA PROTECTION FRAMEWORK IN THE LIGHT OF INTERNATIONAL HUMAN RIGHTS STANDARDS ON PRIVACY

BY

SHARON KUYET YABO

Privacy is not an option and it shouldn't be the price we accept for just getting on the internet -Gary Kovacs

As World Population grows, the World is becoming "transparent" via the Internet, Technology advances and so do Rights. These Rights must be legislated upon and updated as the need for such is indispensable. Amongst these rights is the Right to Privacy. With ubiquitousness of information, the World is now a Global Village therefore the call to define Privacy and Data Protection is very dire.

The Right to Privacy is complex and Ambiguous; one cannot fully exhaust same. However for this discourse, we shall be analyzing privacy in the form of Data using Nigeria as the yardstick, and comparing her laws with that of the International Human Rights Standard on Privacy.

In defining Privacy, one must consider a broad range of loosely allied personal interests. According to Black Laws Dictionary, Privacy is the right that determines the nonintervention of secret surveillance and the protection of an individual's information. Also, the Committee on Privacy in the Information Age argues that the term used in a general way, "includes reference to the type of information available about an individual whether they are primary or derived from analysis.

Furthermore, the International Law provides a Legal framework for Privacy and is outlined in Article 12 and Article 17 of the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) respectively.

What does Data then mean? Data means characters, symbols and binary on which operators are performed by a computer which may be stored or transmitted in the form of electronic signals which is stored in any format or device. What then is Privacy of Data? It can simply be defined as the protection of any Data subject from Data breaches in a data driven world. Internationally, on regional levels, European Union Legislators have enacted the General Data Protection Regulation (GDPR) which aims at protecting all European citizens from privacy and data breaches in an increasingly data driven world and includes all data subject rights.

In Privacy of Data, there are three worthy major stakeholders. They are the Government, Technology/Private Companies and Individuals.

Nigeria Data Protection Regulation.

The Nigeria Data Protection Regulation has been issued by the National Information Technology Development Agency (NITDA) with the following objectives:

1. To safeguard the rights of natural persons to data privacy
2. To foster safe conduct of transactions involving the exchange of personal data
3. To prevent manipulation of personal data and
4. To ensure that Nigerian businesses remain competitive in International trade through the safe guards afforded by a just and equitable legal regulatory framework on data protection.

Accordingly, the scope of this regulation deals with Nigerians living in and out of Nigeria, personal data of natural persons in Nigeria and any natural person entitled under law, contract, or regulation that is in Nigeria at the time being or outside Nigeria. The Regulation is home to 42 sections that clearly spell out their functions and interestingly, these sections are very organized ranging from the objectives to the governing principles of data processing to defining what is lawful to consent of data subject to the objections of a data subject to the rights of a data subject to the local and international cooperation!

Nigeria's Data Protection Regulation in light of International Human Rights standard on Privacy.

Mass Data surveillance and storage have been legitimized based on "war against terrorism". Sadly same reason is used to unlawfully use personal data of individuals. Since Whistleblower, Michael Snowden, the reality of unchecked and indiscriminate use of mass surveillance and Data by UK and US Security Agencies has led to various debates which quickly escalated to the level of the United Nations (UN). While some proponents of increased surveillance point out to the events of 9/11, the opponents of same reason that indiscriminate interception of personal data goes to the very heart of the social contract in modern democracies.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

In January 2014, the following were resolved by the Human Rights Committee on comments on Article 17 of ICCPR and Article 12 of UDHR.

- To make sure all states respect and protect the right to privacy in communication.
- To review methods of legitimization of collecting personal Data and communication interception.
- To effect realization and implementation of this international framework of human rights law.
- The responsibility of technology companies as they may risk the complicity in human rights violation if they follow government requests for surveillance assistance without adequate safeguards.

Under NDPR, amongst the impressive things to note is that the regulation takes into cognizance emerging laws on data protection regulations within the international community and providing for implementation mechanisms and not just protecting Data from hackers, cyber attacks but setting up firewalls, employing data encryption technologies which is primarily the work of anyone in control of Data or Data processing. On the same vein, the regulation states that the right to privacy is for the advancement of data subject and not restricting the safe guards same. Also, it provides for penalty of defaulters of any person who is in breach of any data privacy rights of the data subject.

However, as well put these laws are the implementation mechanisms have been poor. On the 24th and 25th of September, 2019 Taxify otherwise known as Bolt was hacked and peoples' accounts were hacked thereby massive withdrawals were made. The aim of privacy of personal data is to protect the individuals, states and private/technology companies and all interested stakeholders. If these are not protected, regulated and promoted, what then is the safety of one's privacy in this digital age?

To downplay the right to privacy of personal data is to eat the very fabric that covers one's body. The right to privacy is not squarely the responsibility of the states via legislation but involves the stakeholders of personal data to be more pro active and not readily give up information until terms and conditions are explained to them in the simplest form.

Also, implementation mechanisms must be strictly adhered to and this can only be achieved if these laws carry penalties such as sanctions, heavy fines and even imprisonments for failure to adhere to same. It's no secret that when an example is made on three or more natural persons, data controllers, technology companies or even states will be more deliberate on ensuring that the safety of personal data of Nigerians are upheld

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

ANALYSIS OF NIGERIA'S DATA PROTECTION FRAMEWORK IN THE LIGHT OF INTERNATIONAL HUMAN RIGHTS STANDARD ON PRIVACY

BY

CHUKWU JOSHUA CHINEDU

As Abraham Lincoln said, "Democracy is the government of the people by the people and for the people" 1. This is to say that for a state to be one which is of a democratic nature, it must involve actively the populace, by and large. The recognition of fundamental human right takes a veritable position being one key feature of a democratic government. These fundamental human rights are guaranteed every of every state and they are inalienable; they cannot be in any manner deprived of these rights. One of these rights is the right to privacy.2

Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.3 On the international plain, right to privacy is one that is reasonably and diligently recognized as forming part of human existence. This can be seen from the various instruments which provides for the right to privacy. Article 12 of the Universal Declaration of Human Rights 4 prohibits the arbitrary interference with the privacy, correspondence, family or home of any person. In the same vein, Article 17 of the International Convention on Civil and Political Rights provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence. Section 16 of the United Nations Convention on the Right of the Child5 protects the interest of the private life of a child. In Nigeria, the right to privacy has become part of our municipal law by virtue of Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended, 2011)6 which guarantees the right to privacy on the citizen's homes, correspondence, telephone conversations and telegraphic communications. In the light of our study which is that of data privacy, there has so far not been any legislation that directly protects data in Nigeria.

However, since the constitutional provision is one that can be said to be so wide, it is presumed that it seeks to cover data privacy too. Save for the constitutional guarantee of privacy, some other legislations has made for specific or qualified data privacy protection.

One of such is the Consumer Code of Regulations, 20077 which provides that all reasonable steps must be taken to protect customer information against "improper or accidental disclosure " and must ensure that such information is securely stored. In addition to this, the Child Rights Act, 2013 which is a specific legislation seeks to protect the child by limiting access to information in certain circumstances. Section 8 guarantees this right to privacy while Section 205(2) prohibits the publication of any information that will lead to the identification of a child offender.

In the light of the foregoing, a clear analysis of the international instruments which seeks to protect data, it is clear that the current position of the law in regards to right to data privacy in Nigeria remains vague and if taken a bit further, a mirage. This can be construed to be true if there will be consideration of the emerging areas surrounding the conceptualization, data. The aforementioned Section 17 of the International Covenant on Civil & Political Rights(ICCPR) has taken a bit step further since the Committee published General Comment 16 in 1988;8 a step geared towards advancement in data privacy protection. However unfortunate it is, Nigeria is not a signatory to it. The generality of the data privacy protection as is seen under the extant Constitution can be safely agreed to be in conformity with the 1948 Universal Declaration of Human Rights. The question which will intelligently 1948, what does it seek to achieve given the emergence of sophisticated areas which has emerged overtime? It is in this respect that it's of the opinion of this author that the provisions of international instruments which does not reflect adequate protection to data privacy should not be tenable and in no way be one worth adoption. This anomaly which is currently being faced by data privacy in Nigeria has resulted in the breach of the confidentiality of data in reoccurring instances in Nigeria.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

The specific provisions listed earlier has not been adequate to guarantee data privacy as they either apply to a category of persons or they are aimed at protecting customers of the telecommunications sector. This leaves other areas where data sources are, vulnerable. However in the case of Habib Nigeria Bank Ltd. V Fathudeen Syed M. Koya 9the Court of Appeal interpreted the statutory provision accorded to data privacy to include the guarantee of confidentiality on the part of a bank not to disclose their customer's transactional information. Though this has no express provisions in our laws, it is hoped that it serves as a precedent to subsequent litigation on the subject. Also, since the Supreme court has made no pronouncement in this regard, it leaves it open to speculation as the court adopts a more liberal approach to interpretation. In due consideration, the position of the law in regards to data privacy in Nigeria when compared to those of our international counterparts falls below standards.

Conclusively, it is suggested that instruments which provides adequate security to data be adopted and legislative enactments made in this respect. Also, that the constitutional provision of the right of privacy be revisited and be one affected by an expansionary status to address the issues faced by data privacy in contemporary times.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

ESSAY ON PRIVACY AND DATA PROTECTION: AN EXAMINATION OF THE NIGERIA DATA PROTECTION REGULATION 2019 AND ITS IMPLICATIONS FOR SECURITY AND THE ECONOMY.

INTRODUCTION:

Twenty first century economies are digital economies; they rely on data for virtually all their functionalities and/or operations. In fact the very sustenance of every twenty first century economy is hinged on data collection and processing as much as the survival of anemics is dependent on blood transfusion. The relevance of data to any modern economy or organization cannot be overemphasized. Joris Toonders, in his article titled 'Data is the New Oil of the Digital Economy' observed that 'We're in a digital economy where data is more valuable than ever. It's the key to the smooth functionality of everything from the government to local companies. Without it, progress would halt.' This essay examines the salient provisions of the Nigeria Data Protection Regulation 2019 (NDPR) and its possible implications for security and the Nigeria's economy. The essay argued that the NDPR regime has instilled more confidence in data subjects who are now more inclined to volunteer information or their personal data to data controllers without fear of atrocious breach or threat to their lives and property. The essay concluded by recommending the elevation of the NDPR from a subsidiary legislation to a principal legislation amongst others.

EXAMINATION OF THE NIGERIA DATA PROTECTION REGULATION 2019.

Prior to the giant stride taken by the National Information Technology Development Agency (NITDA) on January 25, 2019 in publishing the NDPR, Nigeria never had a single and comprehensive legislation on the protection of personal data. What was hitherto available (save for the constitution) was industrial or sectoral legislation with piecemeal provisions touching on the protection of data and privacy (Perchstone & Graeys, 'A review of the key provisions of the data protection regulation 2019' accessed from Mondaq.com on 23/9/2019).

Some of these legislation include: The Freedom of Information Act 2011 (section 14); The Nigerian Communication Act, 2003 (see regulations such as the General Consumer Code of Practice Regulation and the Registration of Telephone Subscribers Regulations made pursuant thereto); the Child Rights Act, 2003 (section 8); the Cybercrimes (Prohibition, Prevention, etc) Act, 2015; and the National Identity Management Commission Act, 2007.

The 1999 Constitution of the Federal Republic of Nigeria (as amended) equally has a provision touching on data protection and privacy. By section 37 thereof the privacy of Nigerian citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected. Though one of the rights constitutionally guaranteed as a fundamental human right, section 37 is arguably the most limited in scope in that it is inapplicable to foreigners and it would seem that the right does not extend to natural persons of Nigerian descent residing outside the shores of Nigeria. Similarly the right may be curtailed in the interest of defence, public order, public morality, public health or for the purpose of protecting the rights and freedom of other persons (section 45 of the constitution).

In the light of the foregoing and following concerns raised by relevant stakeholders on the issue of privacy and protection of personal data particularly the grave challenge of leaving personal data processing unregulated, the NITDA in January 2019 issued the NDPR with a view not only to ensure the security of lives and property but also to foster the integrity of commerce and industry in Nigeria.

The NDPR takes cognizance of the fact that many public and private bodies have migrated their respective businesses and other information systems online. It recognizes these information systems as critical infrastructure which must be safeguarded, regulated and protected against atrocious breaches hence its stiff provisions and heavy sanctions in the event of breach.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Section 2.6 of the NDPR for instance provides that anyone involved in data processing or the control of data shall develop security measures to protect data; such measures include protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data, protection of emailing systems and continuous capacity building for staff. Section 2.7 further places responsibility on data controllers to execute written contracts with third parties engaged by them to process data and to ensure that such third parties comply with the provisions of the NDPR.

The NDPR in section 2.5 equally provides that any medium through which personal data is being collected or processed shall display a simple and conspicuous privacy policy that the class of data subject being targeted can understand. This is to aid the data subject make an informed decision on whether to give or withhold consent. Where the data subject gives his consent the data controller must ensure that the processing of the data complies with the governing principles enumerated under section 2.1 of the NDPR.

The NDPR imposes stiff penalties for failure to comply with any provision of the Regulation. However this is dependent on the number of data subjects that a company processes. Where the data subjects are more than 10, 000 the penalty is payment of a fine of 2% of Annual Gross Revenue or ten million naira, whichever is greater. Where on the other hand the data subjects processed are less than 10, 000 the penalty is payment of 1% of Annual Gross Revenue or two million naira whichever is greater. The data subject is conferred with many rights under the NDPR. Some of these include right of access to data or copies of data, right to deletion of personal data, right to object to processing, right to restrict processing, right to data portability, right to withdraw consent and right to object to marketing. The NDPR empowers the NITDA to set up an Administrative Redress Panel to receive allegations from data subjects, investigate the allegations where necessary, issue administrative orders and determine appropriate redress (Perchstone & Graeys, supra).

Needless to add that unlike section 37 of the constitution which applies only to Nigerian citizens the NDPR is applicable to all natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent (section 1.2(b)).

IMPLICATION OF THE REGULATION FOR SECURITY AND NIGERIA'S ECONOMY

With the security of their lives and property now enhanced under the NDPR and their confidence thereby restored or stimulated more and more data subjects are likely to now freely volunteer information or give their consent for the collection and processing of their personal data to data controllers. On the other hand investors (both local and foreign) would now be more willing to invest in Nigeria's economy knowing that the requisite data needed for their investments are readily accessible and/or that their investments are protected and safeguarded from nefarious activities of hackers or other atrocious breaches under the NDPR. Indeed, it is a win-win situation for all parties involved. However, all key players must ensure that the provisions of the NDPR are religiously complied with as so doing would not only guarantee the security of data subjects but equally enhance transparency and accountability in data collection and processing and also induce more transactions thereby improving the country's economy.

CONCLUSION/RECOMMENDATIONS

By way of conclusion, the following recommendations are suggested:

1. Given its relevance and enviable record of being the first ever single and comprehensive legislation on the protection of data and privacy in Nigeria, it would be proper if the NDPR is given its appropriate place in the hierarchy of legislation in Nigeria by being elevated from its current status of a subsidiary legislation to a principal legislation. One way of achieving this is by amending the NITDA Act to capture all the provisions of the NDPR. This is equally important as it would forestall a situation where the NDPR would be force to take the back sit each time it is found to be in conflict with any principal legislation for the time being in force in view of the principles of the hierarchy of legislation in Nigeria. It is so recommended.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

Similarly, while it is conceded that the provisions of the NDPR is capable of applying to all natural persons residing in Nigeria it is however doubted if same is possible for Nigerians residing outside of the country and or if same could be enforce by them in the event of breach in their countries of resident particularly as it is trite that no sovereign state can make legislation for another without the latter's concurrence. An amendment of section 1.2(b) of the NDPR deleting the words: "or residing outside Nigeria but of Nigerian descent" is therefore recommended as the said words appear to serve no useful purpose in the Regulation.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

ESSAY ON PRIVACY AND DATA PROTECTION: AN EXAMINATION OF THE NIGERIA DATA PROTECTION REGULATION 2019 AND ITS IMPLICATIONS FOR SECURITY AND THE ECONOMY

BY

ODUDUABASI UMO-ODIONG

In 2013, Edward Snowden uncovered a vast regime of mass government surveillance programmes, opening a global conversation which is still unfolding today. Current and emerging technologies are unavoidably and consequently contributing their bits to make this conversation continuously pertinent. Legislations, lawsuits, activisms, security concerns, advertising and marketing concerns, to mention just a few, are some of the subjects that orbit this conversation which is on **DATA PROTECTION**.

Data protection is primarily concerned with the ways third parties handle information of persons within a given society, country, or continent. The discus of data protection is concerned with how individuals' personal data is collected, processed, shared, stored, accessed, and used. The third parties in this discus means any natural or legal person, public authority, establishment, or any other body than the Data subject (individuals who provide personal data), the Data Controller, the Data Administrator and persons who are engaged by the Data Controller or the Data Administrator to process personal data. The information largely concerned entails individuals' personal data.

Protecting personal data has become a matter of interest for a number of reasons. First, individuals want the sanctity of their privacy upheld. Presumably, this is why the right to privacy is guaranteed in almost every piece of legislation across the globe that deals with human rights, if not all of such legislations. Without having the discussion on data protection, Data Subjects' right to privacy will continued to be meddled with by third parties. These laws also provide avenues for Data subjects whose privacy has been breached to seek redress. Penalty/penalties for such breaches are usually provided.

Secondly, this digital/information age which the world is phasing enables and entails much of data sharing. The advent of social media has been key to a world of an almost unending sharing of personal data. Most, if not all social media platforms only on-board individuals after they have shared their personal data on the platform. For example, to be able sign up on and use the various features of platforms like Facebook, Twitter, WhatsApp, Instagram, amongst other popular social media platforms, an individual has to input his/her personal data. One of the concern that this raises is that, although such inputted data is obtained consensually, how these platforms store and use data after such sign up raises pertinent questions and challenges. One of such challenges is that companies that run these platforms more often than not sell personal data to advertisers.

Furthermore, one can argue that this collecting and sharing individuals' personal data boosts commercial activities. The availability of a collection of individuals' personal data in a given society would aid market research. Such data helps to companies to determine wants, needs, preferences, and taste of individuals. It also aids in disseminating of product information to individuals by using available personal data. The importance of personal data the commercial sector does not preclude its essentiality in fostering digital marketing. The digital market has witnessed a large influx of companies that provide products and services on various digital platforms. This has contributed immensely to the economic growth of countries that welcome such developments. Hence, it would be folly to circumvent the discussion on data protection.

Thirdly, security concerns have created a stimulating dialogue on the data protection discus. The question of whether government should obtain the data of citizens at will is a pertinent one especially with the security challenges such as terrorism, cybercrime that is currently thralling the world. If it is deemed necessary for government to have access to individuals' data, to what extent should such access be limited? This was discussed in the Apple vs Federal Bureau of Investigation's (FBI) case, where the FBI asked apple for the information stored on the iPhone of one of the suspects in the terrorism attack in San Bernardino in 2016. This opened a live debate on the right to privacy, data protection and security needs. This debate remains germane with tenable arguments on each side of the debate.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

From the foregoing, it can be seen that it is quintessential to regulate the information/digital industry, so as to protect individuals/users/the public. This can almost only be done through legislations. Seemingly abstract laws on data protection have been shown to have real life consequences. Take for example, in 2013, Peace Brigade International documented that a combination of massive surveillance and a lack of adequate data protection law facilitated a crackdown on civil society, which witnessed a raid on many human rights defenders' offices, hacking of their computers, and tapping of their phones. It is noteworthy that Kenya's limit on data protection is largely justified by security concerns.

Subject to the discus, several countries have enacted data protection laws. For example, the government of the United Kingdom have passed into law the Data Protection Act 2018, which applies the EU's General Data Protection Regulation (EU) 2016/679 (GDPR) standard. Also, the GDPR which was adopted in 2016 has been key in strengthening fundamental rights of persons across parts of Europe. It has clarified the rules for companies and public bodies in the digital single market.

How far has Nigeria progressed in data protection regulation?

The onus of creating data protection laws, as with all other laws, is on the country and its government. Nigeria's progress in protecting personal data is commendable. Despite the absence of a primary and specific data protection legislation, Nigeria has a subsidiary data protection regulation which was issued by an agency of the federal government. It is known as the Nigerian Data Protection Regulation 2019 (The Regulation), and the agency that issued it is the National Information Technology Development Agency (NITDA).

The Regulation has made notable provisions which this paper will be considering subsequently. The preamble of the Regulation recognises the necessity of electronic communications and data exchange and how they directly affect areas such as education, government, commerce, the public and private sector. It takes cognizance "of emerging data protection regulations within the international community geared towards security of lives and property band fostering the integrity of commerce and industry in the volatile data economy."

It is also conscious of the concerns and contributions of stake holders on the issue of privacy and protection of personal data and the grave challenges that could be faced when personal data is left unregulated.

The Regulation contains relevant and commendable provisions such as the length of time in which companies can retain personal data of individuals, how such data is to be collected and stored. It addresses privacy concerns and rights of individuals. Chapter 2 Section 6 of the Regulation ensures that companies/persons that collect data take adequate steps to protect such data. An advantage of this is that persons would be encouraged to share their personal data when required because of its guaranteed safety. A notable flaw however is that it does not clarify whether government or government establishments have rights to obtain personal data in situations where they can be classified as third parties, and for any possible reason including public safety and security.

Apart from the Regulation, there are also general provisions on data protection in various pieces of legislation and regulations that are industries and sectors specific. They include:

1. Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (The 1999 Constitution), which expressly provides for the right to privacy of individuals in Nigeria. This provision covers individuals' homes, correspondence, telephone and telegraphic conversations. This right is however limited in favour of a reasonably justifiable circumstance such as; in the interest of public safety, defence, public order, public morality, public health, or, whenever it is essential to protect the rights of other persons.
2. The General Consumer Code of Practice Regulation, the Registration of Telephone Subscribers Regulations ('RTS Regulation') 2011, and the Nigerian Communications (Enforcement Process, etc.) Regulation 2005 which were made by Nigerian Communications Commission (NCC) contains provisions that protect personal date.

1. Under section 8 of the 1999 Constitution, the rights under the aforementioned S.37 of the 1999 Constitution are reiterated however, with regards only to 'a child'.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

1. The Cybercrime (Prohibition Prevention, etc.) Act 2015 criminalizes the abuse and misuse of data for fraudulent purposes. It also ensures that have a duty to record, safe keep and protect data for a period of two years.
2. Section 14 of the Freedom of Information Act FOI Act restricts disclosure of personal records without prior consent

In conclusion, the aforementioned laws and more, as well as other sector specific laws provide for data protection in Nigeria. The Regulation, the 1999 Constitution, and all the other laws in no obvious way/s impede economic growth. Nonetheless, only the 1999 Constitution makes reference to a justifiable breach of right to privacy and consequently, a justifiable breach of data protection in the interest of public safety, order, etc. However, the extent of such justification is left unclear by the absence of case laws. All the mentioned laws however provide for adequate data security.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

THE LEGAL FRAMEWORK FOR DATA PROTECTION IN NIGERIA AND POSSIBLE IMPLICATIONS FOR SECURITY AND THE ECONOMY

BY

TOHEEB O. AMUDA.

1.0. INTRODUCTION.

The past few years have witnessed a buzz in the use of the words „data", „big data" and „data protection". With Nigeria keying into this development, the first *Big Data Economy Summit* took place on October 12, 2017 and had representatives from Diamond Bank, MTN, Data Science Nigeria and other nationally prominent organisations.

The use of data or big data has however been around much longer**.** In fact, the earliest records of using data to track and control businesses date back to 7,000 years ago when accounting was introduced in Mesopotamia in order to record the growth of crops and herds.1

What then is Data? *The Cambridge Dictionary* defines data as *"information, especially facts or numbers, collected to be examined and considered and used to help decision-making or information in an electronic form that can be stored and used by a computer."*2

These information can be anything from a name, an address, a photo, videos, audios, images, click streams, online transactions, logs, an email address, bank details, posts on social networking websites, medical information etc. The Forbes Technology Council noted that if This huge availability of data is what the term 'Big Data' refers to. Big data is a term that describes data available in high volume, high velocity, and/or high variety.

How does "who wins or loses a match" in the Premiership on a Saturday affect mobile data usage behaviour? How can Lagos traffic be optimised for effective logistic distribution? These questions and many more are some of the things big data can answer and solve. Companies are now taking advantage of data insights to improve decision-making, enter new markets, and deliver better customer experiences..

In Nigeria, Kudi.ai has developed a chatbot that uses AI to understand user requests, understand user spending habits and prevent fraud. Telecommunications companies such as MTN and Globacom integrate data analysis in their business in order to better understand the customer.

With the importance ascribed to data, it is therefore important that laws be established to protect personal data and safeguard its security.

2.0. LEGAL FRAMEWORK FOR DATA PROTECTION IN NIGERIA.

The following are legislations that impacts data protection in Nigeria and form the Nigeria data protection legal framework: 1. The 1999 Constitution of the Federal Republic of Nigeria (as amended): Data protection and privacy is an extension of the fundamental right of citizens to privacy guaranteed under Section 37 of the Constitution.

2. The Nigeria Data Protection Regulation 2019 („the Regulation"). The Regulation was issued by the National Information Technology Development Agency (NITDA) on the 25th of January, 2019. It is made by virtue of the NITDA Act 2007, the principal Act. The Regulation repealed the Data Protection Guidelines 2013 („the Guidelines"). The Regulation aims at protecting the personal data of all Nigerians and non-Nigerian residents in Nigeria.

The Regulation provides for the rights of the Data Subject,4guides and put in check the Data Controller (the person or persons who determine how personal data is processed)5 and provides for the roles of the Data Protection Officer (a person designated by the Data Controller to implement the Regulation).6

The Regulation provides and set the guidelines for the transfer of Data to third party countries and also provides for penalties for failing to comply with the Regulation.

3. The Freedom of Information Act 2011: The Freedom of Information Act is not a data protection law, but section 14 of the Act protects personal data. The section restricts disclosure of personal records without obtaining consent.7

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*

4. The Nigerian Communications Act 2003: By virtue of the powers conferred by the NCA 2003 on the Nigerian Communications Commission (NCC), regulations that touch on data protection in the telecommunications industry have been made by NCC. These regulations are the General Consumer Code of Practice Regulation, the Registration of Telephone Subscribers Regulations ('RTS Regulation') 2011, and the Nigerian Communications (Enforcement Process, etc.) Regulation 2005.

5. The Child Rights Act 2003: The Act through section 8 reinforces the constitutional rights of the child, including privacy rights under section 37 of the 1999 Constitution. 6. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Cybercrimes Act): Under the Cybercrimes Act, abuse and misuse of data for fraudulent purposes are criminalised. Service providers have a duty of record retention and data protection. 7. The National Identity Management Commission Act 2007 (NIMC Act): By virtue of section 31 of the NIMC Act, the National Identity Management Commission (NIMC) powers include the power to provide for the collection, collation, and processing of data and any other relevant information.

The Credit Reporting Act 2017: In the financial sector, the Act amongst other things protects the confidentiality rights of data subjects, including the right to consent and the right to accurate personal information.

9. The National Health Act 2014: In Nigeria"s health sector, the Act requires health service providers to keep a record of patients" personal information by storing every user"s health records safely and in strict confidentiality.

10. Consumer Protection Framework (the "Framework") 2016: One of the provisions of this Act as introduced by the Central Bank of Nigeria (CBN) is that it protects consumer assets and privacy.

3.0. POSSIBLE IMPLICATIONS FOR SECURITY AND THE ECONOMY.

With the enormous data being generated in the world, estimated at 2.5 quintillion bytes every day,8this huge value of data is increasingly becoming attractive to governments, companies and also hackers. Data is now subject to cyber threats. In September 2018, there were reports that a cyber-attack exposed Uber's data from 57 million customers and drivers.9Facebook also had its share of cyber-attack in September 2018 as 90 million Facebook user accounts were exposed by a security breach in the UK.10

Coming home, due to a growing number of internet connected devices such as smartphones in Nigeria, the implication of data and data protection, as it relates to security is critical. If a huge volume of data gets to the wrong hands, this breach can wreak havoc to individual finances and the economy. Withdrawals can be made from bank accounts including widespread identity theft, impersonation amongst others.

This is why there is a general obligation to ensure the security of personal data. The NDPR requires that anyone involved in data processing or the control of data must have security measures to protect such data. These security measures include protecting systems from hackers, setting up firewalls and storing data securely etc. 11

Data can also be used as a shield in national security. The tracking and combating of terrorist group can be achieved through analyzing the data generated from their activities, which leave traces via phone calls, e-mail and logs from those networks.

Leveraging data can also boost Nigeria"s economy. The ability to draw information from millions of different sources is especially beneficial to developing countries with a predominance of rural areas and poor institutional capacity, as it has the potential to better lives by forecasting poverty and shared prosperity through mobile phone data, using satellite imagery to monitor and map electrification of rural areas, to better understand the targets of financial inclusion and climate smart agriculture, to name a few. Having a stable and broad data protection legal framework is therefore critical to attracting investments. A stable and elaborate data protection regime will ensure the availability and accessibility of more data which in turn results in effective service delivery and boosts investors" confidence in the economy.

4.0. CONCLUSION

The 21st century is an era of data. Although there is no single principal data protection law in Nigeria which covers all areas of data, the author submits that economic growth can be achieved with the proper implementation and enforcement of all the available laws highlighted above. A careful concerted effort by data protection authorities is therefore required.

[1] *Boyd D, It's Complicated: the social lives of Networked Teens (Yale University Press 2014) 57.*

[2] *Nigerian Data Protection Act, 2023, s2(1)(a) & s 31(1)(a)*

[3] *Mariam Arain and others, 'Maturation of the adolescent brain' (2013) 9 Neuropsychiatric Disease and Treatment 449.*

[4] *Zuboff S, The Age of surveillance capitalism: the fight for a human future at the new frontier of power (Profile Books 2019)*

[5] *TechHive Blog,'Social Media and Data Privacy: A Nigerian Perspective' (15 March 2023) https://www.techhive.ng/social-media-data-privacy-nigeria/ accessed 31 August, 2025.*