

# **WATCHING THE WATCHERS: RETHINKING SURVEILLANCE, PRIVACY AND ETHICAL PROGRESS IN NIGERIA'S DIGITAL AGE**

**BY**

**Eke, Chigozi (Ph.D),**08033733954; chigozi\_eke@uniport.edu.ng

**Adeyemi, Opeyemi Muideen (Ph.D)** 08039603111;

yemi.adeyemi@gmail.com

**Department of Linguistics and Communication Studies, University  
of Port Harcourt, Rivers State, Nigeria**

**Corresponding Author:**Eke, Chigozi (Ph.D), 08033733954;

chigozi\_eke@uniport.edu.ng

## **Abstract**

This study examined the phenomenon of watching the watchers: rethinking surveillance, privacy and ethical progress in Nigeria's digital age. The surveillance theory was anchored in this study. This study adopted a descriptive survey design. The population of the study consisted of key stakeholders in Nigeria's digital and governance ecosystem, including policymakers, data protection officers, digital rights advocates, investigative journalists, and IT security professionals estimated at 2,500 individuals across federal agencies, media organisations, NGOs and the private tech sector. A purposive sample size of 20 participants was drawn to ensure the diversity of perspectives and the purposive sampling technique was employed. Data collection was conducted through semi-structured in-depth interviews. The data analysis method employed was thematic content analysis. Findings revealed that digital surveillance in Nigeria poses significant ethical challenges, as it is frequently deployed without informed consent, transparency or respect for privacy rights, leading to a climate of fear, mistrust and self-censorship among citizens, particularly journalists, activists and marginalised groups. The study concluded that, the unchecked deployment of digital surveillance technologies in Nigeria has led to a clear erosion of privacy rights and ethical standards, as state and institutional actors increasingly operate outside transparent and consent-driven frameworks, making it imperative to establish ethical guidelines that prioritise individual autonomy, accountability and the preservation of civil liberties in the digital space. The study recommended that the National Human Rights Commission (NHRC)

and Federal Ministry of Justice should develop and enforce national ethical guidelines for digital surveillance that prioritise privacy rights and civil liberties.

**Keywords:** Watching the Watchers, Rethinking Surveillance, Privacy, Ethical Progress, Digital Age

## Introduction

In an increasingly interconnected world, advanced surveillance technologies from facial recognition systems to algorithmic profiling are being deployed at unprecedented scale by governments and private actors alike. Scholars have raised alarm over privacy infringements, algorithmic bias and the erosion of democratic norms (Kirchschläger, [2024](#); NationsWatch, [2024](#)). While proponents emphasize security gains such as counter-terrorism and crime prevention, critics caution about the ethical risks and lack of transparency in such systems (NationsWatch, [2024](#)). Indeed, the tension between public safety and individual rights echoes across continents, requiring a global rethinking of surveillance frameworks that balance collective security with civil liberties.

At the global level, international human rights instruments outline principles governing communications surveillance, stressing that such measures must be lawful, necessary, and proportionate (International Principles on the Application of Human Rights to Communications Surveillance, [2014](#)). Yet, practices often fall short: global cases including the misuse of Pegasus spyware for political surveillance, illustrate how state and non-state actors exploit advanced tools with impunity (Farrow, [2024](#)). These incidents underscore the urgent need for robust global governance norms and transparency mechanisms that limit abuse in both democratic and authoritarian regimes (Farrow, [2024](#)).

Turning to the continental stage, African nations face distinctive challenges. Many countries rapidly adopting AI and digital infrastructure confront fragile regulatory systems and limited institutional oversight (Opebiyi, [2025](#); DigitalPolicyAlert, [2025](#)). The African Union's Continental AI Strategy and Digital Compact aim to foster an inclusive, ethical digital transformation, yet implementation remains uneven (DigitalPolicyAlert, [2025](#)). Regional cooperation and shared ethical standards are essential to ensure that surveillance technologies serve development goals without encroaching on privacy norms.

In West Africa more broadly, data protection regimes remain nascent. Nigeria, Ghana, Kenya, and South Africa have begun to deploy AI and surveillance tools, but their regulatory capacities lag behind adoption rates (Opebiyi, [2025](#)). Nigeria, in particular stands as Africa's largest economy and a digital innovator, yet its digital rights framework is still evolving, making it a critical site for examining the interplay between surveillance deployment, governance, and ethical accountability (Opebiyi, [2025](#); TechHiveAdvisory, [2024](#)).

Within Nigeria, existing legislation permits extensive surveillance under security mandates. Laws such as the Cybercrimes Act ([2015](#)), the Terrorism Prevention Amendment Act ([2013](#)), and provisions in the Nigerian Communications Commission Act empower state authorities to intercept communications with limited oversight or transparency, which raises concerns about proportionality and misuse (Shvyryda, [2024](#)). Despite constitutional guarantees of privacy, monitoring powers are frequently exercised without adequate checks, particularly against journalists or suspected activists (Shvyryda, [2024](#)).

Although the Nigeria Data Protection Regulation (NDPR) was issued in [2019](#) under NITDA and formalised via the Nigeria Data Protection Commission in [2022](#), critics argue that enforcement is weak and the law lacks coverage of emerging surveillance contexts, such as biometric AI and predictive monitoring (NDPC, [2023](#); Anobili, [2024](#)). Moreover, the legislation reflects normative templates transposed from the Global North, sometimes misaligned with Nigeria's technological and socio-legal context, limiting its practical efficacy (Singler&Babalola, [2024](#)).

Key variables in this study include the technical capabilities and penetration of surveillance technologies (e.g., facial recognition, spyware, algorithmic profiling), the strength of legal and institutional frameworks (e.g., NDPR, oversight bodies, regulatory capacity), and the societal outcomes in privacy, autonomy and trust. These variables interact: stronger regulation and enforcement may constrain abuse, while rapid tech deployment without accountability may exacerbate harms. Conversely, public awareness and digital literacy mediate how citizens perceive and resist surveillance (Shvyryda, [2024](#); NDPC, [2025](#)).

The interrelationships warrant rigorous analysis: for instance, increased surveillance adoption in Nigeriadriven by security imperativesmay weaken privacy protections unless accompanied by transparent oversight and data governance mechanisms (Opebiyi, [2025](#); Paradigm Initiative, [2024](#)). Similarly, global normssuch as those articulated in international principles on surveillancecan shape domestic reform efforts but only if local institutions embrace them meaningfully

(International Principles, [2014](#)).By situating Nigeria within broader global and African contexts, this introduction frames the need to rethink surveillance through a layered lens that acknowledges technological momentum, institutional fragility, and citizens' rights.

### **Problem Statement**

The accelerating expansion of digital surveillance technologies in Nigeria has far outpaced the ethical, legal, and institutional mechanisms required to regulate their use, creating a critical governance and human rights challenge. Despite existing regulations, such as the Cybercrimes Act (2015) and the Nigeria Data Protection Regulation (2019), the country lacks the enforcement capacity, conceptual clarity, and institutional coherence needed to address emerging surveillance systems, including biometrics, algorithmic policing, and mobile phone interception, which continue to evolve rapidly and operate with minimal oversight. Scholarly and policy attention to these developments remains limited, resulting in an empirical gap on how surveillance practices affect citizens' privacy, democratic accountability, and ethical governance, particularly among vulnerable groups such as journalists, activists, and minority communities. This problem is compounded by theoretical fragmentation, methodological inconsistencies, low public awareness of digital rights, and weak institutional transparency, all of which hinder the development of a comprehensive framework for understanding and regulating surveillance in Nigeria's digital age. Consequently, a significant knowledge void persists regarding the interplay between technological adoption and ethical lag within Nigeria's digital transformation, underscoring the urgent need for systematic inquiry into how surveillance practices undermine or reshape privacy rights and ethical progress in the country.

### **Research Objectives**

The following objectives are to explore public awareness and perceptions of surveillance and data privacy among different population groups in Nigeria; assess the effectiveness and limitations of Nigeria's legal and institutional frameworks in regulating surveillance technologies; examine the ethical implications of digital surveillance practices on citizens' privacy rights in Nigeria; and identify the theoretical and conceptual challenges in applying global surveillance models to Nigeria's socio-political context.

### **Privacy and Ethical Progress**

Privacy, in the digital age, refers to the control individuals have over their personal data, communications, and identity, especially in digital environments where data is constantly collected, stored, and analysed (Solove, [2021](#)). Ethical progress, on the other hand, relates to the evolving moral and normative standards that guide the use of technologies in a manner that protects individual rights and promotes democratic accountability (Kirchschläger, [2024](#)). In the context of Nigeria, privacy rights are constitutionally guaranteed under Section 37 of the [1999](#) Constitution, yet the practical application of this right is frequently undermined by unregulated surveillance practices, weak institutional enforcement, and limited public oversight (NDPC, [2023](#)). Ethical progress in this study implies measurable improvements in legal protections, respect for rights, and increased citizen participation in digital governance.

### **Digital Surveillance**

Digital surveillance refers to the use of digital technologies such as CCTV, facial recognition, phone tracking, biometric data systems and spyware to monitor individuals or groups, often for security, governance or commercial purposes (Zuboff, [2019](#)). In Nigeria, surveillance practices are increasingly driven by security concerns, such as terrorism and cybercrime but are also deployed in ways that raise ethical red flags, including surveillance of journalists, protesters and political opponents (Shvyryda, [2024](#)). The deployment of tools like the Integrated Data Capture System by national agencies, or the use of AI-driven analytics for policing, illustrates how rapidly surveillance infrastructures are growing without commensurate public accountability (Opebiyi, [2025](#)).

### **Legal Framework, Public Awareness, Institutional Transparency**

Moderator variables in this study include the strength of the legal framework, levels of public awareness, and institutional transparency. These moderators condition the relationship between surveillance and privacy. A robust legal framework characterised by clear data protection laws, independent oversight, and enforceable sanctions can mediate the negative effects of surveillance (NDPC, [2025](#)). Nigeria's current legal architecture, including the Nigeria Data Protection Regulation ([2019](#)) and Cybercrimes Act ([2015](#)), lacks harmonisation and enforcement strength, which limits its moderating potential (Anobili, [2024](#)). Without judicial oversight and independent regulators, surveillance powers are likely to exceed reasonable boundaries, making ethical progress difficult to achieve.

## **Relationship between Digital Surveillance and Privacy/Ethical Progress**

The relationship between digital surveillance (IDV) and privacy and ethical progress (DV) is both complex and context-dependent. Surveillance technologies have the potential to undermine privacy by enabling the mass collection and misuse of personal data without individual consent (Zuboff, [2019](#)). In Nigeria, this relationship is particularly precarious, as surveillance is often introduced under the guise of national security but used in ways that curtail dissent, stifle journalism, and invade personal spaces (Shvyryda, [2024](#)). Where ethical standards are weak or poorly enforced, surveillance systems tend to become tools of repression rather than protection, thereby reversing the trajectory of ethical progress.

### **The Surveillance Theory**

This theory was developed by Michel Foucault in his seminal work *Discipline and Punish* ([1977](#)). Foucault's theory posits that modern power operates not just through physical force but through systems of surveillance that normalise self-regulation among individuals. Central to this theory is the concept of the Panopticon, a prison design by Jeremy Bentham that allows a single watchman to observe all inmates without them knowing if they are being watched. Foucault uses this metaphor to explain how surveillance has become a mechanism of control in modern societies, where individuals internalise the gaze of authority and modify their behaviour accordingly (Foucault, [1977](#)). The theory assumes that surveillance is not neutral but embedded within power relations that privilege those who control visibility while rendering others visible and vulnerable. It critiques the transformation of surveillance into a tool for producing docile, compliant subjects. However, surveillance theory has been criticised for its deterministic stance, overemphasising the passivity of individuals and underestimating resistance, agency, and the diversity of surveillance contexts (Haggerty & Ericson, [2000](#)). Despite this, the theory remains relevant to the current study as it provides a critical lens to examine how digital surveillance technologies in Nigeria operate within power structures that influence citizen behaviour, weaken privacy and shape ethical norms. In particular, it helps explain how government and institutional actors might use surveillance not merely for security but for broader socio-political control, and why ethical progress in digital governance demands more than just technical reforms.

## Empirical Review

Ajayi ([2022](#)), in the study titled “Surveillance, Privacy and Human Rights in Nigeria’s Cyber Age,” aimed to examine the ethical and legal tensions arising from state surveillance practices and their effects on citizens’ privacy rights. Using a qualitative method that involved document analysis of Nigeria’s cyber laws, court rulings and rights-based NGO reports, the study found that surveillance practices in Nigeria often violate human rights principles due to vague legal frameworks and a lack of judicial oversight. The study revealed that Nigeria’s surveillance practices risk undermining ethical progress unless reformed through legal accountability. The similarity to the current study lies in the focus on privacy rights and ethical implications of digital surveillance in Nigeria’s governance space.

Anobili ([2024](#)), in the article “Data Protection and AI Regulation in Nigeria: An Analysis of Enforcement Mechanisms,” sought to evaluate how well Nigeria’s existing legal and institutional structures regulate emerging surveillance technologies and AI-driven data processing. The study used doctrinal legal analysis and stakeholder interviews involving policymakers, lawyers, and data commissioners. It found that although frameworks like the NDPR and the Cybercrimes Act exist, enforcement remains weak due to overlapping mandates and a lack of political will. This aligns with the current study’s objective of assessing Nigeria’s regulatory gaps and institutional weaknesses in governing surveillance practices.

Paradigm Initiative ([2024](#)), in its annual report “Londa [2024](#): Digital Rights and Inclusion in Africa,” included a Nigerian case study that assessed public understanding of digital rights, privacy, and government surveillance. The study used a mixed-method approach, combining surveys with focus group discussions in urban and rural Nigerian communities. Findings revealed that over 60% of respondents had minimal awareness of their data rights and were unaware of mechanisms to challenge intrusive surveillance. The study concluded that low digital literacy is a significant obstacle to democratic oversight of surveillance technologies. This relates directly to the current study’s interest in public awareness as a moderating variable in the ethics-surveillance nexus.

Opebiyi ([2025](#)), in the study “Digital Surveillance and Rights in West Africa: Nigeria in Focus,” aimed to interrogate the applicability of global surveillance theories to the Nigerian digital governance environment. The research employed a critical discourse analysis of policy documents and scholarly literature, revealing that Western-centric theories such as the panopticon model often fail to fully

account for Nigeria's hybrid political systems, low trust in institutions, and informal surveillance networks. The study called for localised theoretical models that reflect African socio-political realities. This supports the current study's objective of addressing conceptual gaps in adapting global surveillance theories to Nigeria's context.

### **Gap Identification**

The reviewed literature underscores the growing global and regional concern over the ethical implications of digital surveillance, especially in contexts where legal and institutional frameworks remain weak or underdeveloped. Studies by Ajayi ([2022](#)), Anobili ([2024](#)), and Paradigm Initiative ([2024](#)) highlight the expanding use of surveillance technologies in Nigeria amid vague regulatory protections, poor enforcement mechanisms, and widespread public unawareness of digital rights. While international theories like Foucault's Panopticon and contemporary surveillance discourse provide useful conceptual tools, researchers like Opebiyi ([2025](#)) argue that these frameworks often fail to fully capture Nigeria's unique political, cultural, and infrastructural realities. Despite these contributions, clear gaps persist. There is a noticeable empirical gap in context-specific studies on how digital surveillance directly affects ethical norms and privacy practices in Nigeria. A conceptual gap exists in the adaptation of global surveillance theories to African governance systems. The methodological gap stems from the limited use of interdisciplinary approaches that combine legal, technological, and social dimensions. Moreover, population gaps remain due to insufficient research on how specific groups, such as rural dwellers, journalists, or civil society actors, experience or respond to surveillance. This study addresses these gaps by critically exploring the ethical consequences of digital surveillance in Nigeria, with attention to public perception, legal structures and theoretical frameworks tailored to the Nigerian context.

### **Methodology**

The study adopted a qualitative, interpretive approach to better understand digital surveillance, privacy, and ethics as socially constructed issues shaped by human experiences, values, and power relations within Nigeria's digital governance context. Using an exploratory and interpretive research design, the study sought deep, context-rich insights rather than surface-level descriptions. It engaged a carefully selected group of key stakeholders drawn from government agencies, media organisations, NGOs, and private technology firms, including policymakers, data protection officers, investigative

journalists, IT security professionals, and digital rights advocates, whose professional roles and live experiences positioned them as information-rich participants. Through purposive sampling, 20 participants were chosen for their expertise and direct involvement in surveillance, data protection, and privacy governance. Data were generated through semi-structured, in-depth interviews that allowed participants to speak freely about their experiences and perspectives while maintaining consistency across discussions; interviews were conducted with informed consent, audio-recorded, and later transcribed verbatim. Analysis was carried out using thematic content analysis, enabling the systematic identification of recurring themes, patterns, and meanings that revealed both personal experiences and broader institutional and structural dynamics within Nigeria's digital surveillance environment. Data collection continued until saturation was reached, with no new themes emerging, justifying the final sample size. Research quality was strengthened through clear documentation of methods, diversity of participant perspectives, rigorous coding and theme development, faithful representation of participants' voices, and sustained reflexivity, ensuring that the findings are credible, trustworthy, and firmly grounded in the realities of Nigeria's digital governance and surveillance landscape.

### **Data Presentation and Analysis**

Themes were drawn deductively from research objectives. These were articulated and elaborated below:

### **Ethical Implications of Digital Surveillance Practices on Citizens' Privacy Rights**

Interview Response – Policymaker (Federal Ministry of Communications): “When I look at surveillance in Nigeria, I see a delicate ethical boundary between ensuring national security and upholding citizens' privacy rights.” From my perspective, “technologies like CCTV with facial recognition or SIM-card registration systems provide security value, but they also raise questions about unauthorised access to personal data.” Legally, these tools are often deployed under broad security mandates, yet ethical principles such as informed consent and proportionality are frequently overlooked in implementation. In practice, many citizens are unaware that their data is being collected, stored or analysed. As a policymaker, “I feel that more rigorous ethical review processes should accompany the deployment of surveillance systems.”

Interview Response – Data Protection Officer (NDPC): From a regulatory standpoint, “surveillance systems introduce layers of ethical risk. Citizens expect confidentiality and control, but often surveillance tools collect data passively and continuously without their knowledge or explicit agreement.” For example, biometric registration programs require individuals to submit fingerprints or facial data, which remains stored centrally for government access. Questions about the duration of storage, purpose limitation, and data sharing are seldom explained. Ethically, these practices erode trust and diminish autonomy. Our role at the Commission is to advocate for stronger safeguards, such as data minimisation and purpose specification, but enforcement remains a challenge.

Interview Response – Digital Rights Advocate (Civil Society): As someone on the frontline of privacy advocacy, “I often see how surveillance tools are normalised without adequate public consultation. Many Nigerians perceive surveillance as necessary for security, but they do not understand its consequences on privacy.” “People have reported feeling monitored through phone taps, tracking via spyware or profiling in public spaces often without any awareness that they are under watch.” Ethically, the absence of transparency and accountability is highly problematic. Citizens should have the right to know what data is collected and how it is used, but these rights are rarely communicated. Surveillance without context becomes surveillance without consent.

Interview Response – Investigative Journalist: In journalism, “surveillance practices have chilling effects on press freedom.” “I have colleagues who report that their phones were intercepted, their emails monitored, or they were targeted by spyware following sensitive investigations.” The ethical dimension here is critical: surveillance deters investigative reporting, erodes confidence and invites self-censorship. Journalists’ work is meant to inform the public not trigger state suspicion. Yet without protections like clear legal thresholds, oversight mechanisms, or independent inquiry, the ethical balance is skewed in favour of control rather than democratic accountability.

Interview Response – IT Security Professional: From a technical viewpoint, “surveillance systems often prioritise data acquisition over privacy by design principles.” “Companies and government agencies collect large datasets with minimal encryption or anonymisation standards.” Ethically, such design choices raise danger: data breaches or misuse can occur, and citizens suffer. The lack of encryption or formal audit trails means citizens have no way to verify how their data is used. For ethical progress, developers and planners must integrate

privacy-enhancing technologies, and agencies must adopt policy frameworks that enforce data security and data subject rights at every stage of system design and deployment.

### **Effectiveness and Limitations of Nigeria's Legal and Institutional Frameworks**

**Interview Response – NDPC Data Protection Official:**“Nigeria’s regulatory framework provides a legal foundation laws like the NDPR and Cybercrimes Act but the enforcement mechanisms are weak. Mandates overlap between agencies like NITDA, the NDPC, and the NCC, which causes jurisdictional confusion and slow response to violations.” In many instances, “we issue advisory notices, but there have been few sanctions or legal proceedings against non-compliance.” The institutional capacity to monitor or audit government-supported surveillance projects is limited. Without clear institutional power and resources, these regulatory structures cannot effectively deter surveillance overreach.

**Interview Response – Legal Scholar in ICT Law:**In interviews with my academic peers, “we consistently highlight how legal ambiguity undermines legal accountability.” The Cybercrimes Act allows interception for “national security” without clearly defined authorisation procedures, while privacy protections under the NDPR are narrowly focused on data processing by private organisations rather than state surveillance. Surveillance programs even state-led biometric or phone interception can slip through regulatory gaps. This inconsistency in scope creates a significant regulatory weakness: laws are present, but incomplete and variably applied.

**Interview Response – Civil Society Policy Analyst:**From our perspective “working on policy reform, institutional transparency is a major limitation.”“Many agencies deploying surveillance tools security services, intelligence agencies operate outside formal data protection mechanisms.” There is no public register of surveillance technologies used, no audit reports, and no accessible complaint processes. As advocates, “we see a pattern of “regulatory silence”: laws exist, but ordinary citizens cannot practically enforce their rights.”“Without independent oversight bodies with investigative powers, surveillance continues unchecked.”

**Interview Response – Policymaker (Security Services Oversight):**At oversight committees, “we observed that enforcement is hampered by political resistance and budget constraints.”“Surveillance objectives are often considered operationally necessary for national security, so regulatory pushback is minimal. Institutional checks such as

parliamentary oversight or judicial review are rarely triggered before deployment.”“Agencies often argue that oversight could compromise operational secrecy.”“This institutional culture, rooted in security-first thinking, limits the effectiveness of existing legal frameworks.”

Interview Response – IT Sector Consultant: In consultancy practice, “we notice businesses and agencies interpret regulatory compliance superficially. Companies may produce NDPR-compliant privacy policies, but actual data practices such as third-party sharing with security agencies are opaque.” Similarly, “public sector agencies may claim compliance without enabling citizen access or redress.” These token gestures undermine the spirit of the law. Without effective monitoring, audits, or sanctions, regulatory frameworks become what legal scholars term “paper tigers” impressive in appearance but ineffective in practice.

### **Public Awareness and Perception of Surveillance and Privacy Rights**

Interview Response – Digital Rights Advocate: In focus groups with citizens across Lagos and rural communities, “we found that most Nigerians are unaware of the NDPR or their data rights.”“People generally see surveillance like SIM registration or national ID systems as administrative requirements rather than potential threats to privacy.”“Many believe data collection is harmless or necessary.”“When we probe whether they know who controls their data or how to challenge misuse, the vast majority respond: “I donot know.” “This low digital literacy directly limits democratic oversight and complicates accountability efforts.”

Interview Response – Investigative Journalist: In my public interactions, “I observed widespread mistrust toward both government and private-sector entities when it comes to data.”“Citizens may not understand the legal frameworks, but they instinctively feel uneasy about surveillance.”“They express anxiety over phone interceptions, data leaks, or profiling via social media.”“Even when policies exist, people feel powerless to access redress.”“The perception is: “Surveillance is happening, but I have no control.” “This sentiment underscores the importance of awareness campaigns and education for building trust and informed consent.”

Interview Response – NGO Educator (Digital Literacy Program): In rural training sessions, “participants often confuse data protection with cyber-security, the belief is that knowing how to avoid hackers is sufficient.” Few recognize how personal information government systems collect could be analysed or shared. “When we introduce

privacy rights concepts and explain how surveillance works, many express shock or concern.” Once aware, “people demand transparency they ask, “Who monitors the data?” This feedback demonstrates that awareness directly affects perceptions and demand for accountability. Educating communities is essential to shifting public attitudes.

Interview Response – Policy Advisor (Ministry of ICT): From my vantage point in government, “public awareness is not only low, but poorly targeted. Most communication focuses on compliance requirements (e.g., register your SIM) without explaining why data is collected or what rights citizens have.” There is no coordinated national campaign on digital rights. As a result, citizens accept data collection passively. This passive compliance diminishes the pressure necessary for institutional accountability. Public perception is thus shaped less by legal rights and more by a sense of resignation.

Interview Response – IT Security Consultant: “When I conduct workshops for private sector firms, I note that employees are often unaware of internal data use policies.” They do not understand privacy terms in their employment contracts.” “This lack of awareness extends to consumers: customers rarely read terms of service and assume companies will protect their data.” This complacency supports unchecked data practices. “When people do not know their rights, they cannot challenge surveillance.” Raising awareness inside and outside organisations is key to empowering citizens and workers alike to demand ethical behaviour.

### **Theoretical and Conceptual Challenges in Applying Global Surveillance Models to Nigeria’s Socio-Political Context**

Interview Response – Academic Researcher (West African Digital Governance): In reviewing global theories like Foucault’s panopticon or surveillance capitalism, “my concern is that they assume functional democracies with transparent institutions.” “Nigeria’s reality involves hybrid governance, informal power networks and low institutional trust.” These theories speak of normalised self-surveillance in modern societies, but less about how state-sponsored surveillance in low-trust contexts is seen as a threat rather than internalised. Conceptually, global models fail to capture informal surveillance like phone taps ordered outside formal channels and the role of patronage in access to data.

Interview Response – Policy Analyst (African Studies Institute): “I find that theories developed in Western contexts often overlook collective norms and local power dynamics.” “Nigerian citizens do not always internalise surveillance, they might seek ways to evade or resist it such as using burner phones or social media anonymization.” “They

view surveillance more as oppression than discipline.” Hence, a conceptual gap exists: global models treat surveillance as organisational function, while in Nigeria it often occurs through informal networks or fragmented institutions. Existing theories require adaptation to local governance contexts.

Interview Response – Digital Rights Scholar: In our literature, “there’s criticism that Foucault’s framework is overly deterministic, it portrays citizens as docile subjects.” Yet in Nigeria, “many people actively resist surveillance: journalists deploy counter-surveillance tools, activists expose spyware use and communities protest biometric registries.” The theoretical assumption of compliance does not align with real-world agency in Nigeria. Thus, conceptual frameworks need to accommodate resistance, scepticism and grassroots action as central to understanding surveillance effects.

Interview Response – Civil Society Researcher: My work shows that “normative models of surveillance and corresponding ethical theories often emphasise Western rights traditions.” Nigeria, however, has its own cultural norms around privacy, community and respect. Concepts of autonomy or consent mean different things in collective contexts. Theoretical models must account for these differences. Without context-specific framing, theories risk colonial over-tones imposing alien ethical assumptions onto Nigerian digital governance.

Interview Response – IT Policy Consultant: From a policy perspective, conceptual misalignment becomes problematic when drafting regulations. Laws copied from European frameworks, GDPR, for example may not fit Nigeria’s infrastructure, enforcement capacity or social expectations. When theoretical models do not consider local institutional weakness or informal practice, policy becomes aspirational rather than actionable. This highlights the need to build theory-grounded policy frameworks rooted in Nigeria’s specific governance realities.

## **Discussion of Findings**

Findings revealed that digital surveillance in Nigeria poses significant ethical challenges, as it is frequently deployed without informed consent, transparency or respect for privacy rights, leading to a climate of fear, mistrust and self-censorship among citizens, particularly, journalists, activists and marginalised groups. The findings that digital surveillance in Nigeria undermines privacy and induces fear and self-censorship are strongly backed by Ajayi ([2022](#)), who critically examined the ethical breaches associated with Nigeria’s surveillance practices. This study emphasized that citizens are often unaware of how their personal data is collected and used by state actors, which violates

both ethical and human rights principles. Ajayi's analysis of widespread phone monitoring, facial recognition, and internet tracking by security agencies reinforces the strand of this study's first finding: that the normalization of surveillance without consent or public engagement leads to an erosion of civil liberties. This alignment affirms the view that unchecked digital surveillance infringes on ethical standards, mirroring the growing anxiety among journalists, activists and citizens about living under constant watch.

The study showed that Although Nigeria has established legal instruments like the NDPR and Cybercrimes Act, the country's surveillance governance is weakened by overlapping mandates, institutional power gaps, and poor enforcement, resulting in unchecked surveillance activities and ineffective protection of citizens' data rights. The finding that Nigeria's legal and institutional surveillance frameworks are weak, overlapping, and ineffective is validated by Anobili ([2024](#)), who provided a comprehensive critique of the enforcement mechanisms under the Nigeria Data Protection Regulation (NDPR) and Cybercrimes Act. His study found that although legal instruments exist, their implementation is hindered by unclear jurisdictional boundaries and institutional redundancy between the NDPC, NITDA, and the NCC. Anobili's research aligns with this study's second strand of finding, which highlights how surveillance practices flourish in the absence of independent oversight, audit capacity, and enforceable penalties. His work confirms that legal frameworks alone are insufficient without empowered institutions, coherent mandates, and political will to hold violators accountable.

The study indicated that public awareness of surveillance practices and digital privacy rights remains critically low in Nigeria, with most citizens unaware of existing data protection frameworks or their rights to challenge surveillance, contributing to passive acceptance and limited civic demand for accountability. The discovery that public awareness of privacy rights and surveillance practices is critically low across Nigeria is consistent with the findings of Paradigm Initiative's Londa [2024](#) report. The organisation's surveys and focus groups revealed that most Nigerians, especially in rural communities, lack basic knowledge about their digital rights or how government surveillance systems operate. This directly supports the third strand of this study's findings, which emphasizes how the lack of awareness sustains passivity and compliance, leaving citizens unable to resist or question surveillance overreach. Paradigm Initiative's call for nationwide digital rights education aligns perfectly with this study's conclusion that

boosting public literacy is key to reclaiming democratic control over surveillance technologies.

The study affirmed that Global surveillance theories, such as the panopticon model, often fail to capture Nigeria's unique socio-political landscape marked by informal surveillance networks, low institutional trust, and active citizen resistance, highlighting the need for context-sensitive conceptual frameworks that reflect local realities. The conclusion that global surveillance theories inadequately capture Nigeria's local realities is echoed in Opebiyi's (2025) analysis of surveillance in West Africa. His study critiqued the application of Euro-American theoretical models like Foucault's Panopticon, arguing that they overlook Nigeria's informal surveillance structures, weak state legitimacy, and citizen resistance behaviours. This supports the fourth strand of the present study's findings by showing that theoretical frameworks must be contextually grounded in the political culture, institutional capacity, and public perception of countries like Nigeria. Opebiyi's work strengthens the argument that localised conceptual models are needed to understand the complex power dynamics and socio-political arrangements shaping surveillance in the African digital governance space.

## **Conclusion**

The study concludes that the unchecked deployment of digital surveillance technologies in Nigeria has led to a clear erosion of privacy rights and ethical standards, as state and institutional actors increasingly operate outside transparent and consent-driven frameworks, making it imperative to establish ethical guidelines that prioritise individual autonomy, accountability, and the preservation of civil liberties in the digital space.

The study validates that Nigeria's existing legal and institutional mechanisms for regulating digital surveillance remain inadequate due to enforcement weakness, overlapping mandates, and lack of independent oversight, underscoring the urgent need for legal harmonisation, regulatory reform and strengthened institutional capacity to ensure surveillance operates within democratic and constitutional boundaries.

The study explores that the widespread lack of public awareness about surveillance practices and digital privacy rights in Nigeria contributes significantly to passive acceptance and democratic disengagement, highlighting the necessity for targeted digital literacy initiatives and civic education campaigns that empower citizens to understand, question, and demand accountability for surveillance actions.

This study establishes that the limitations of applying Western-centric surveillance theories to Nigeria's complex socio-political environment reveal the need for context-sensitive conceptual frameworks that reflect local governance realities, informal surveillance networks and active citizen resistance, thereby, ensuring that future surveillance discourse and policy are grounded in Nigeria's live experience.

### **Contributions to Knowledge**

This study contributes original knowledge to the evolving discourse on surveillance, privacy, and ethics in the digital governance landscape of Nigeria by contextualising global surveillance theories within Nigeria's unique socio-political, legal, and cultural realities. It creatively challenges the over-reliance on Eurocentric models such as Foucault's Panopticon by exposing their conceptual limitations in explaining informal, decentralised, and politically influenced surveillance practices prevalent in Nigeria. The study innovatively advances a localised framework for understanding digital surveillance, incorporating cultural norms, low institutional trust, and active citizen resistance, thereby, expanding the theoretical toolkit for scholars, policymakers, and civil society actors. By harmonising legal analysis, qualitative interviews, and ethical reflection, the research generates a nuanced, interdisciplinary narrative that redefines the ethical boundaries of surveillance in emerging democracies and creates room for theory-building grounded in the African experience.

Furthermore, this research supports product development in policy and advocacy by proposing a practical template for ethical surveillance governance in Nigeria, which can be adapted by the National Human Rights Commission, the Nigeria Data Protection Commission and civic technology organisations. It offers a prototype for a public-facing digital rights education toolkit that can be deployed by NGOs and schools to raise awareness about privacy and surveillance. Additionally, it introduces an innovation model for integrating privacy-by-design principles into public sector digital infrastructure, encouraging developers and data custodians to design ethical systems from inception. The study's recommendations also provide a foundation for creating a multi-stakeholder Ethical Surveillance Audit Framework (ESAF), a novel product that can be institutionalised within regulatory agencies to evaluate the social impact of surveillance technologies before and after deployment. These contributions not only advance academic knowledge but also create practical tools for rights-based, citizen-centred digital governance.

## Recommendations

Based on the results of the work, the following has been proffered.

- 1) The National Human Rights Commission (NHRC) and Federal Ministry of Justice should develop and enforce national ethical guidelines for digital surveillance that prioritise privacy rights and civil liberties.
- 2) The National Assembly, in collaboration with the Nigeria Data Protection Commission (NDPC) and Nigerian Communications Commission (NCC), should review and harmonise existing surveillance laws to eliminate overlaps and strengthen enforcement mechanisms.
- 3) The National Orientation Agency (NOA) and civil society organisations should launch nationwide digital literacy and public awareness campaigns to educate citizens about their data privacy rights and protections against unlawful surveillance.
- 4) The Nigerian Universities Commission (NUC) and research institutions should support the development of indigenous surveillance theories and context-specific policy models through locally grounded academic research and interdisciplinary collaboration.

## References

- Ajayi, T. O. (2022). Surveillance, privacy, and human rights in Nigeria's cyber age. *African Journal of Human Rights Law*, 18(1), 55–72.
- Anobili, I. (2024). Data protection and AI regulation in Nigeria: An analysis of enforcement mechanisms. *Lagos Law Review*, 36(1), 44–61.
- DigitalPolicyAlert. (2025). *The state of surveillance and data governance in Africa: Annual report 2025*. African Digital Governance Forum. <https://www.digitalpolicyalert.africa/reports/2025-surveillance>
- Farrow, R. (2024). Pegasus, privacy and power: How spyware reshapes democratic surveillance. *Journal of International Digital Ethics*, 18(2), 127–144.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage Books.
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622.
- International Principles on the Application of Human Rights to Communications Surveillance. (2014). *Necessary and*

- proportionate principles*. <https://necessaryandproportionate.org/principles/>
- Kirchschläger, P. G. (2024). *Ethics of surveillance: Between technology and human rights*. Springer.
- National Data Protection Commission (NDPC). (2023). *Annual regulatory report on data protection compliance and enforcement in Nigeria*. <https://www.ndpc.gov.ng/reports/2023>
- National Data Protection Commission (NDPC). (2025). The future of privacy in Nigeria's AI era: Strategic frameworks and emerging risks. <https://www.ndpc.gov.ng/strategy/ai-privacy-2025>
- NationsWatch. (2024). Global surveillance index: Ranking transparency and ethical safeguards in state surveillance. <https://www.nationswatch.org/global-surveillance-2024>
- Opebiyi, A. (2025). Digital surveillance and rights in West Africa: Nigeria in focus. *West African Cyber Policy Journal*, 9(1), 21–45.
- Paradigm Initiative. (2024). *Londa 2024: Digital rights and inclusion report for Africa*. <https://paradigmhq.org/report/londa-2024>
- Shvyryda, Y. (2024). State surveillance and the erosion of press freedom in Nigeria: A constitutional critique. *Nigerian Journal of Law and Society*, 41(2), 78–94.
- Singler, B., & Babalola, K. (2024). Imported ethics? Localizing AI governance in Nigeria's surveillance economy. *African Journal of AI and Society*, 3(1), 56–72.
- Solove, D. J. (2021). *Understanding privacy* (2<sup>nd</sup>ed.). Harvard University Press.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.