Policy Brief

ANALYSIS OF THE ENFORCEMENT OF NIGERIA'S CODE OF PRACTICE FOR INTERACTIVE COMPUTER SERVICE PLATFORMS/INTERNET INTERMEDIARIES

PARADIGM INITIATIVE

Credits

Author

Sani Suleiman

Reviewed by

Khadija El-usman and Thobekile Mtimbe

Design and Layout:

Bakinde Mathias Gomes

374 Borno Way, Yaba, Lagos, Nigeria
Email: media@paradigmhq.org
www.paradigmhq.org

Table of Contents

INTRODUCTION

In 2022, the National Information Technology Development Agency (NITDA) issued the Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries, a regulatory instrument designed to address online harms, improve platform accountability, and strengthen Nigeria's digital ecosystem. Paradigm Initiative (PIN) conducted an initial assessment of the Code shortly after its release, identifying ambiguities, enforcement gaps, and areas requiring refinement to align with constitutional and human rights standards.

Building on that early analysis, PIN subsequently convened a Digital Policy Engagement Series, bringing together civil society actors, legal experts, technologists, and digital rights advocates to critically examine the Code's implementation prospects. This policy brief synthesises the insights emerging from that engagement, providing a granular examination of the Code's provisions and their practical implications for rights-respecting digital governance in Nigeria.

This assessment acknowledges the NITDA's recently submitted first regulatory compliance report (Compliance Report (2024) on the Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries), containing noteworthy figures on platform adherence, takedown practices, and user complaints. While the report signals progress in institutionalising reporting obligations, it also underscores persistent inconsistencies in how platforms interpret their duties and how the Agency evaluates compliance. While this brief is not focused on the report itself, it offers valuable perspective that can inform recommendations on how NITDA can enhance transparency in its operations and make the Code more human-rights-centric

GRANULAR ASSESSMENT OF THE CODE OF PRACTICE

1. Enforcement Architecture and Missing Safeguards

The Code assigns extensive responsibilities to platforms under Part I and Part II, including requirements to remove prohibited content, enforce community guidelines, and provide accessible grievance channels. However, enforcement is entirely platform-centric, with no complementary obligations imposed on the government to ensure transparency, due process, or proportionality in enforcement.

The absence of independent oversight mechanisms means that the Code relies on NITDA's internal processes, raising concerns about self-assessment and potential regulatory overreach. Stakeholders highlighted that these risks undermine public trust and could create ambiguity around accountability pathways.

2. Ambiguities in Part V (Disinformation and Misinformation)

Part V attempts to address harmful content, but several clauses lack precision or conflict with existing legislation. For instance, Section 7(a) exempts users who merely "transmit" harmful content without editing or modifying it. Participants at the engagement series noted that this provision undercuts accountability, allowing harmful content to proliferate while limiting liability. Others argued that the section conflicts with parts of the Cybercrime Act, creating interpretive uncertainty for regulators and platforms.

[1] NITDA Code Response Memo
[2] Compliance Report (2024) on the Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries (CoP for ICS

3. Reporting Standards and NITDA's First Compliance Report

The Code requires Large Service Platforms (LSPs) to submit annual compliance reports under Section 10, but the Code does not specify the depth or disaggregation needed. The first compliance report submitted by NITDA illustrates this gap: while it provides overall figures for removals, flagged content, and enforcement actions, it lacks a breakdown of:

- Voluntary removals
- Removals following NITDA intervention
- Removals by court order
- User appeals and reversals
- A breakdown of the thematic areas of reports removed

Without these disaggregated categories, it is difficult for the public or oversight bodies to assess whether takedown actions are rights-respecting, proportionate, and procedurally sound.

4. Lack of Precise Criteria for "Harmful Content"

The Code repeatedly refers to "harmful," "prohibited," and "illegal" content without providing operational definitions or thresholds for these terms. Participants in the policy engagement series emphasised that effective content regulation requires a multi-factor assessment, considering:

- The speaker's profile and influence
- Context, tone, and intent
- The medium used (video, text, audio)
- Proximity to real-world harm

This absence of clarity increases the risk of over-enforcement, including takedowns of lawful speech, particularly around political expression and dissent.

5. Weak Dispute Resolution Mechanisms

The Code does not propose any specialised or independent body for resolving disputes arising from takedowns, account restrictions, or government removal requests. Without a tech-focused tribunal or appeal body, disputes rely on slow judicial processes that are ill-suited to the fast-paced nature of digital content moderation.

6. Evidence Preservation Failures

While Section 4(1) mandates the removal of unlawful content within 24 hours, it does not mandate the preservation of such content for evidentiary purposes. This undermines both regulatory oversight and the ability of victims to seek redress through law enforcement or civil litigation. The lack of a retention clause is a significant procedural flaw.

RECOMMENDATIONS TO NITDA

Nigeria's digital regulatory framework must balance safety, innovation, and human rights. Based on the findings, stakeholder inputs, and PIN's analysis, the following actions are essential:

1. Establish Independent Oversight and Transparency Mechanisms

Nigerian government through relevant agencies must adopt a multi-stakeholder oversight model, including civil society, academia, and technical experts. Annual compliance reports should be made public, with independent audits verifying:

- The accuracy of takedown data
- The legality of government requests
- The due process standards applied by platforms

Transparent oversight is vital for accountability on both state and platform actions. NITDA needs to develop or make things transparent in terms of how they identify the publications they take down. What are the basis of the request for the takedown, not just the numbers.

2. Clarify Legal Definitions and Align the Code with Existing Law

Part V should be revised to remove redundancies and ensure consistency with the Cybercrime Act, Evidence Act, and constitutional protections for speech. Ambiguous sections—especially Section 7(a) - should be replaced with a due diligence standard that promotes responsible sharing without criminalising ordinary users.

3. Reinforce Clear State Obligations and Safeguards

Issues around

- Requiring court orders for intrusive data requests
- Ensuring transparency in content removal directives
- Publishing quarterly logs of regulatory interventions

Without government accountability, platform obligations alone cannot protect rights.

4. Strengthen Reporting Standards and Data Disaggregation

NITDA should develop standard reporting templates requiring platforms to provide detailed breakdowns of the following:

- Content removals by category
- Appeals, reinstatements, and error rates
- Government-requested actions
- Automated vs. human moderation outcomes

This enhances monitoring, comparability, and the usefulness of research.

5. Introduce a Technology Dispute Resolution System

NITDA must collaborate with the Judiciary to establish a specialized digital rights tribunal or a fast-track mechanism staffed by legal and technical experts to hear appeals on account bans, content takedowns, and regulation-related disputes. Further to this, NITDA should develop a reporting pipeline where ordinary citizens can report harmful content, as these remedies must be accessible to everyone

CONCLUSION

The Code of Practice represents an important step toward strengthening Nigeria's digital governance framework. However, without more precise definitions, independent oversight aside from NITDA's, and balanced government accountability, it risks reinforcing opacity rather than fostering trust.

This policy brief, grounded in PIN's initial analysis, expanded through the Digital Policy Engagement Series, and contextualised by NITDA's first compliance report, underscores the need for a recalibrated framework that protects Nigerians from online harm while upholding constitutional freedoms. A more transparent, rights-respecting, and evidence-driven regulatory approach will position Nigeria as a leading voice in digital governance on the African continent.

374 Borno Way, Yaba, Lagos, Nigeria
Email: media@paradigmhq.org
www.paradigmhq.org

PARADIGM INITIATIVE