Data & Policy (2025), 7: e12
doi:10.1017/dap.2025.1

RESEARCH ARTICLE

Digital policy and Nigeria's Platform Code of Practice: towards a radical co-regulatory turn

Vincent Obia

School of Journalism, Media and Communication, University of Sheffield, Sheffield, UK
Email: v.a.obia@sheffield.ac.uk

Received: 02 February 2024; **Revised:** 25 October 2024; **Accepted:** 06 December 2024

Keywords: co-regulation; digital policy; platform regulation; Nigeria; NITDA Code of Practice

Abstract

This study examines Nigeria's National Information Technology Development Agency Code of Practice for Interactive Computer Service Platforms as one of Africa's first push towards digital and social media co-regulation. Already established as a regulatory practice in Europe, co-regulation emphasises the need to impose duties of care on platforms and hold them, instead of users, accountable for safe online experiences. It is markedly different from the prior (and existing) regulatory paradigm in Nigeria, which is based on direct user regulation. By analysing the Code of Practice, therefore, this study considers what Nigeria's radical turn towards co-regulation means for digital policy and social media regulation in relation to standards, information-gathering, and enforcement. It further sheds light on what co-regulation entails for digital regulatory practice in the wider African context, particularly in terms of the balance of power realities between Global North platforms and Global South countries.

Policy Significance Statement

This article interrogates Nigeria's contemporary digital regulatory practice, highlighting the shift towards platform co-regulation as represented by the 2022 National Information Technology Development Agency Code of Practice. It gives particular attention to the balance of power realities that policymakers across the Global South must consider as they draft digital regulatory policy. It also outlines the implications of platform co-regulation for countries like Nigeria and provides suggestions on regulatory provisions that can make co-regulation in these countries more realistic. Overall, the study will enable policymakers to better understand the limitations of digital co-regulatory policy in a country like Nigeria, the need not to be too trusting of platforms, and the importance of consistency in policymaking.

1. Introduction

On 26 September 2022, the Nigerian government, through the National Information Technology Development Agency (NITDA), signalled a new direction for social media regulation in the country. What embodied this new direction was a regulatory document called the *Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries* (hereafter called "the Code"). It was introduced by NITDA, a federal agency set up in 2007 to, in part, regulate information technology practices, activities, and systems in Nigeria (see Section 6(a) of the NITDA Act, 2007). NITDA instituted the Code after the 2020

#EndSARS movement, which Twitter (now X) played a huge role in facilitating (see Obia, 2020 https://blogs.lse.ac.uk/medialse/2020/11/11/endsars-a-unique-twittersphere-and-social-media-regulation-in-nigeria/), and the subsequent ban of X in 2021. It aims to set best practice guidelines for digital platforms, which means it serves as a co-regulatory instrument targeted at social media and other internet platforms instead of the previous practice of targeting users (Obia, 2023a). It also aligns with the call, contained in the 2019 African Declaration of Principles on Freedom of Expression and Access to Information, for African countries to ensure that digital intermediaries mainstream human rights standards into their processes (see Principle 39(3) of the Declaration).

Despite this call in the 2019 African Declaration of Principles, examples of co-regulatory instruments in Africa are almost non-existent. We can point to a few instances such as Ethiopia's 2020 Hate Speech and Disinformation Prevention and Suppression Proclamation and Tanzania's 2020 Electronic and Postal Communications Regulations, both of which combine direct user regulation with co-regulation (see Articles 7 and 8 of the Ethiopian Proclamation and Sections 7 and 14 of the Tanzanian Regulation). The NITDA Code adds to these existing regulatory documents and serves as one of the first policies wholly articulated in co-regulatory terms, underscoring its "radicalness" and significance in the African context. More importantly, it represents a bold attempt by an African country to regulate powerful Big Tech platforms in the Global North, bringing to the fore tensions in the power asymmetry between Global North platforms and Global South countries. The Nigerian example, therefore, presents a unique opportunity to study one of Africa's first forays into co-regulation, an area on which the literature is silent. This is what I aim to address in this study by asking two questions:

1. What does the Code say about Nigeria's radical turn towards co-regulation?
2. How does this turn interplay with broader digital balance of power considerations?

My argument ultimately is that the radical co-regulatory turn is ill-fitting for Nigeria because of the power asymmetry between Global North platforms and Global South countries—a reality that also applies to other African countries that may see Nigeria's co-regulatory turn as a democratic example to emulate. To demonstrate this argument, I begin the study by reviewing the literature on the power (a)symmetry that informs how countries across the Global North and South relate with Big Tech platforms before considering the previous regulatory trend on digital and social media regulation in Nigeria. Following this is a discussion of the method and an analysis of the Code in line with relevant entries in other documents. I conclude the study by examining the implications of Nigeria's radical turn towards co-regulation.

2. Co-regulation and balance of power between platforms and countries across the global north and south

Co-regulation, as used in this article, is defined as a regulatory system where states mandate platforms to regulate user behaviour (mainly through moderation) or face sanctions for non-compliance (Marsden and Meyer, 2019). It prescribes a structure based on regulated self-regulation, where platforms are deputised as governing agents under a regional or national entity (Balkin, 2018). An example of a place where co-regulation exists is Europe, which has turned away from American absolutist ideas on free speech to introduce the Digital Markets Act (DMA) and the Digital Services Act (DSA)—two regulatory instruments that represent one of the most comprehensive applications of co-regulation to the business and content aspects of digital platforms (Manganelli and Nicita, 2022). Co-regulation, therefore, suggests a hierarchy, one where states occupy a position of power over platforms to mandate certain standards and enforce compliance.

The question of power is my central point of interest, and it is one that scholars have explored (Hardy, 2014), with suggestions that platforms have become too powerful to regulate (Nyabola, 2023). We see this in the description of social media platforms as oligopolies that can undermine alternative governance approaches that question the capitalist model on which they are founded (Fuchs and Sandoval, 2015).

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

This points to their business model, which has made US platforms such as Meta, Google, Amazon, Apple, and Microsoft the five most profitable companies in the world (Nyabola, 2023). DeNardis and Hackl (2015) also speak of platforms as "information choke points" that serve as the de-facto global public sphere. They also exist as "institutions of governance, complete with generalized rules and bureaucratic features of enforcement" (Kaye, 2019, 16)—leading Klonick (2018, 1602) to describe them as "the New Governors of online speech."

My objective, therefore, is to highlight the political and economic influence that platforms wield, and how co-regulation underscores the power asymmetry between platforms and states. The few studies that have considered this in the African context tend to describe the power asymmetry in terms of digital colonialism (Coleman, 2019; Kwet, 2019). Coleman (2019), for instance, speaks of data protection in Africa, noting that tech platforms usually come into Africa as monopolies with the ability to determine how the digital ecosystem operates. And although African countries are now instituting data protection laws in an attempt to rebalance the power equation, there is nothing stopping Big Tech platforms from disregarding these laws since they have violated data protection instruments in Global North countries (Coleman, 2019). What this shows is the precarious balance of power between Global North countries and platforms, and if this is the case for the Global North countries, then the asymmetry in power relations between Global South countries like Nigeria and the major platforms is far more pronounced (Takhshid, 2022).

We can point to examples in Latin America, where Bizberge et al. (2023) acknowledge the power asymmetry that exists, noting that the digital ecosystem involves global players (e.g., tech platforms) who occupy positions of dominance. It is perhaps why Kwet (2019, 4) asks: "Can the countries of the Global South shape their own digital destiny?" In this light, co-regulation in Nigeria as represented by the NITDA Code can be seen as an attempt by Nigeria to shape its digital destiny. But as Nyabola (2023, 467) notes, there is still "a major gap" for countries like Nigeria "that experience the effects of [platforms] but are unable to take action in response." This gap is one that I consider by interrogating Nigeria's turn towards co-regulation.

3. Nigeria's digital policy trend and the turn towards co-regulation

By introducing the Code in 2022, the Nigerian government, through NITDA, signalled a move from direct user regulation, which is defined as overt punitive regulation targeted at user conduct or the restriction of user access to platforms (Nakaayi, 2022). These are measures that form the default regulatory practice for most African countries (Gumede, 2016). They underscore the concept of regulatory annexation, which is the extension of standards, principles, and norms meant for one frame of reference (e.g., broadcasting) to another (e.g., social media) (Obia, 2023a). We see this in the way that users in Nigeria are held liable as publishers (Obia, 2021), who are accountable for online posts just as journalists bear responsibility for media content. Regulation of this kind includes three items, which I discuss below: laws that target freedom of expression in digital spaces (Olukolu et al., 2019), instruments that use online harms as an excuse to institute punitive policies (De Gregorio and Stremlau, 2021), and technical measures such as internet bans and filtering to stifle popular online discourse (Elega et al., 2023).

When it comes to laws that target freedom of expression, Vareba et al. (2017) show that internet regulation in Nigeria has always been articulated through a bouquet of legal instruments such as the 2015 Cybercrimes Act and the now-defunct 2015 Frivolous Petitions Bill, which broadly implicate digital rights and muzzle anti-establishment voices. These measures are usually justified on national security grounds (Moses et al., 2022) and are therefore counterproductive since they negatively affect freedom of expression. This is worsened by how vaguely worded social media policy documents tend to be (Nakaayi, 2022), as we find in places like Nigeria (Obia, 2023a), Chad (Kalemera et al., 2020), Uganda (Rukundo, 2018), and the broader African landscape (Gumede, 2016).

In relation to combatting harmful digital content, there is some agreement on the need for action. Fombad (2022), for instance, outlines the way that the fake news phenomenon can negatively affect democracies in Africa. Consequently, African countries, including Nigeria, have introduced legal and technical means seeking to address fake news and hate speech (Garbe et al., 2021). The regulatory trend,

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

however, suggests that concerns related to online harms have been used as justification to introduce internet censorship across the Global South (De Gregorio and Stremlau, 2021). In Nigeria, this underscores the politics of regulation, where social media regulation, couched in the public interest, actually exists to protect the concerns of the ruling political elite (Obia, 2021). It explains why regulation in Nigeria is characterised by citizen distrust, since people fear that regulation, supposedly meant to combat online harms, will be used to muzzle critical views that the government deems to be offensive (Abdullateef, 2021).

This fear of criticism and overt dissent is also what influences the trend of internet shutdowns and other restrictive measures, pointing to ulterior motives in regulatory practice (Chari, 2022). These shutdowns are inherently political since they are usually introduced during highly politically sensitive periods such as elections or protests (Wagner, 2018). Shutdowns in Africa began with the Arab Spring, when Egypt introduced bans to suppress anti-government demonstrations (Gerbaudo, 2013). They have since spread to several African countries (Marchant and Stremlau, 2019). Nigeria joined the list in 2021, when the government imposed a 7-month ban on X, what Elega et al. (2023) see as the beginning of digital authoritarianism in the country. Beyond bans, there is also evidence that the government has engaged in coordinated inauthentic behaviour (Bradshaw et al., 2020) and other means of stifling free online spaces.

Despite the established practice described above, the indication in recent times is that the Nigerian government has moved towards greater engagement with social media platforms (Apanpa, 2023). This suggests a shift, at least in nominal terms, from direct user regulation targeted at user conduct to something more closely tied to platform regulation. It is a turn from the previous regulatory trend to a system that the NITDA Code establishes, one that is based on co-regulation. What makes the turn particularly radical is the unequal balance of power that countries like Nigeria face in their dealings with the major Global North platforms. This is the central point of the questions I seek to answer.

4. Method

To answer my research questions, I employ policy analysis as a method. My approach draws from textual analysis of policy documents, which is heavily used in mass communication law research and represents one of Philip Bobbitt's six archetypes of constitutional argument (see Carter, 2017). The textual analysis was informed by Lodge and Wegrich's (2012) regulatory analysis framework, which sees regulation as a manifestation of differing interests, making it anything but apolitical. The framework itself stands on three main analysis points that Lodge and Wegrich (2012) call the regulatory regime: standard-setting (with a focus on the objectives of regulation), enforcement (which examines how behaviour modification is to be achieved), and information-gathering (which considers how regulators gather data on whether standards and enforcement are being achieved).

By complementing the textual analysis with the regulatory analysis framework, I analyse the content of the Code to highlight how it foreshadows a new relationship between Nigeria and digital platforms. In particular, I explore the power asymmetry between Nigeria and Global North platforms to problematise the operational practicability and enforcement of the Code.

5. Findings: analysis of the NITDA code

In this section, I present the outcome of my analysis of the NITDA Code (2022) (a copy of the Code is available at the NITDA website: https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf). Altogether, I discuss seven items, the first five of which focus on the standards in the Code, with the remaining two addressing information-gathering and enforcement. The first three items address research question one, and the latter four items research question two.

5.1. Emphasis on co-regulation and mis/disinformation

Signed into effect on 26 September 2022, the Code represents the most explicit attempt at co-regulation in Nigeria. One of its objectives is to "adopt and apply a *co-regulatory* approach towards implementation

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

and compliance" (emphasis mine). Another objective is to "set out best practices required of Interactive Computer Service Platforms/Internet Intermediaries." What we see here is a shift from the previous pattern of direct user regulation, where the government regulates social media users directly through laws like the 2015 Cybercrimes Act or the Criminal or Penal Code. Regulatory proposals such as the draft Internet Falsehood Bill have also emphasised direct user regulation. By contrast, the NITDA Code shifts the regulatory focus to digital platforms, requiring them to abide by certain obligations.

Part I of the Code begins by outlining these obligations. First, platforms are expected to comply with Nigerian law; hence, they effectively come under Nigerian courts and are to obey court orders when it comes to releasing data for official investigations, for instance (NITDA Code, Part 1, § 1). The protections for which platforms are obligated largely centre around protecting users from online harms, implying that the Code has more of a harms-based as opposed to a rights-based approach. The Code defines online harm as "action or inaction with a reasonably foreseeable risk of having an adverse physical or psychological impact on individuals." However, the focus points to both individual and systemic harms. This is because the Code (in another one of its objectives) seeks to "set out best practices [for platforms] that will make the digital ecosystem safer for Nigerians and non-Nigerians in Nigeria," while also viewing information technology systems as critical infrastructure to be regulated and protected from online harms. The final objective of the Code is to "set out measures to combat online harms such as disinformation and misinformation."

Provisions on misinformation and disinformation are more clearly outlined in Part V of the Code. There, the Code notes the need for a "multivariate" solution and, in line with the co-regulatory emphasis, specifies the responsibilities that digital platforms bear in dealing with complaints, moderation, and research. As a result, platforms are to "work collectively with stakeholders to combat disinformation and misinformation." The stakeholders include data scientists, indigenous academics, researchers, media organisations, journalists, civil society organisations, and government agencies. The Code also requires platforms to invest in research on the causes of and solutions to mis/disinformation (NITDA Code, Part V, § 2). Platforms are further expected to provide researchers with access to data (excluding proprietary data) to facilitate research around combatting mis/disinformation (NITDA Code, Part V, § 3). The Code also encourages platforms to acquaint themselves with the contextual peculiarities of mis/disinformation in Nigeria (NITDA Code, Part V, § 1). This is a nod to the fact that NITDA ascribes transborder co-regulation to the Code, expecting it to cover digital platforms that operate in Nigeria (or have users in Nigeria), even if they are headquartered outside the country—I expand on this below.

Beyond research and moderation, the Code identifies media literacy as a way to address mis/disinformation. Here, platforms are either to "independently organise" (NITDA Code, Part V, § 4) or "collectively collaborate" (NITDA Code, Part V, § 5) with stakeholders (e.g., indigenous media organisations) to organise and execute media literacy programmes on areas such as critical thinking and dealing with online falsehoods. This suggests an emphasis on the protectionist approach to media literacy as opposed to the empowerment approach (Lunt and Livingstone, 2012). The fact that platforms are to organise media literacy programmes (whether independently or collaboratively) could also mean that initiatives will be tailored more according to platform interests, given that media literacy funders have considerable influence on programme objectives (Edwards et al., 2023). This point also applies to the stipulation on platform funding for research, something that NITDA should be wary of. Overall, one thing that is lacking is the "how." The Code encourages platforms to invest in research and media literacy but does not state the parameters. For instance, how much should platforms commit or what percentage of their revenue should go into research and media literacy funding? The Code is also thin on details regarding where and how media literacy programmes should be delivered.

There are further questions to be asked around the special focus that NITDA has given to mis/disinformation by dedicating one out of six parts to it. If the objective is to protect users from online harms, then there are surely other types of harms (e.g., hate speech, online harassment, and coordinated inauthentic behaviour), which might be eclipsed as a result of the focus on mis/disinformation—something which the Code alludes to in recognising that problematic content is not only harmful; it can also be unlawful.

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

5.2. Moderating harmful *vs.* unlawful content

The Code differentiates between harmful and unlawful content. It designates harmful content as "content which is not unlawful but harmful," and unlawful content as "any content that violates an existing law in Nigeria." The Code gives greater attention to unlawful content. For instance, while virtually all the Sections in Part I apply to unlawful content, only Section 4 in Part II speaks to harmful content directly. In that Section, platforms are expected to take some steps before moderating harmful content. First, upon receiving a notice or complaint, platforms are to "carry out a risk assessment to determine whether a content is harmful" (NITDA Code, Part II, § 4).

This risk assessment is on a micro or case-by-case basis, and so does not require the macro-level resources needed for a systemic risk assessment. In carrying out the risk assessment, platforms are to consider the harm that the particular content poses, its level of physical or psychological risk to children or adults, its reach, and the socio-cultural context in Nigeria. All these could take some time depending on the situational realities or harm in question (e.g., misinformation could be harder to settle than hate speech)—pointing to the fact that enforcement is reactionary as opposed to proactive.

When it comes to addressing unlawful content, platform moderation duties are more specific. Here, risk assessments are not needed; platforms only have to confirm that the content in question violates any Nigerian law. Notices for moderating unlawful content can come from "an Authorised Government Agency," and platforms have to acknowledge and remove the content within 48 hours (NITDA Code, Part I, § 2). In Section 3, users can also request that unlawful content be removed as soon as reasonably practicable, and in Section 4, anyone (users or non-users) can request that non-consensual and intimate content be removed within 48 hours. Again, this buttresses the co-regulatory emphasis in the Code. It is a departure from the practice of holding users liable for unlawful content; the new direction is to mandate platforms to sanitise digital spaces, with users empowered to make complaints.

Once these complaints or notices are "substantiated," platforms can remove them without fear of liability (NITDA Code, Part, I, § 5). For users, a notice is substantiated when it is submitted with the URL of the unlawful content. For government agencies, the requirements are more stringent—they are to provide not just the URL, but also the timestamp, a clear statement of the basis of the legal claim and supporting rationale, and the portion of the law that the content violates. This shows that NITDA sees the need to apply constitutionality and legality to the way claims are made. It, however, leaves room for interpretation, since there is a tendency for the law, which the said content violates, to be interpreted in several ways, particularly in Nigeria, where ambiguity allows for openness in interpretation (see Obia, 2023b, for instances of vagueness in the Cybercrimes Act).

5.3. Additional responsibilities for platforms

There are other procedural requirements that platforms are expected to follow, further underscoring the co-regulatory emphasis of the Code. For instance, platforms are required to preserve removed content (NITDA Code, Part II, § 5) and display a label to show that a piece of content has been removed and the grounds for the removal (NITDA Code, Part II, § 6). In Section 7 of Part II, platforms are expected to preserve information on any person no longer using a platform "as required by applicable law." This provision is potentially inconsistent with the right to be forgotten provisions in the Nigeria Data Protection Regulation (NDPR), 2019, which states that a "Data Subject shall have the right to request the Controller to delete Personal Data without delay" (Nigeria Data Protection Regulation, Part 3, § 9; also see this open call by *Paradigm Initiative* (2022), a digital rights organisation, which notes that Part II, § 7 of the NITDA Code contravenes the Nigeria Data Protection Regulation: https://paradigmhq.org/an-open-call-to-nitda-to-review-the-updated-code-of-practice/). It also clashes with the Nigeria Data Protection Act, 2023, which says data subjects have the right to request "rectification or erasure of personal data" (Nigeria Data Protection Law, Part IV, § 34(1)(v)). It is noteworthy that the NDPR was also issued by NITDA.

Part V of the NITDA Code continues with additional requirements for platforms. They are to provide tools for users to easily report mis/disinformation. They are also to work with fact-checkers to identify mis/disinformation and take steps to provide the correct information based on credible sources. This

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

shows that platforms are to take on significant fact-checking duties. In cases of false information reported to platforms by a government agency, information that is likely to cause violence or that threatens the unity, peace, and security of Nigeria, platforms are further required to caution the publisher in addition to removing the content. They are also to ensure that removed content is not found in searches and feeds. There is also an additional requirement for platforms to close accounts and sources that amplify mis/disinformation. I note the likelihood that this can be misapplied, given that the Code does not define what classifies as an account that amplifies mis/disinformation.

5.4. Transborder application

In terms of user scope, the Code applies only to those who are resident in Nigeria, including non-Nigerians. This means it does not apply to Nigerians living abroad. However, in relation to platform scope, the Code applies to "all Interactive Computer Service Platforms/Internet Intermediaries, including entities that are their subsidiaries, affiliates, and agents in Nigeria" (NITDA Code, Scope and Application). This shows that the Code implicates all digital platforms, including Meta, Google, Amazon, Microsoft, and X, that have users in Nigeria. It underscores the Code's transborder application, which indicates that NITDA seeks to extend its influence across the world, unmindful, it would seem, of the balance of power realities that I discussed in the literature review. This balance of power points to the unequal power relations that Global South countries face when it comes to dealing with Big Tech platforms, which draw from the influence they wield as global corporations and the structural advantage of being headquartered in rich and powerful Global North countries.

The transborder application of the Code is further established in its Definition Section. The Code defines Interactive Computer Service Platforms as "any electronic medium or site" where user-to-user interaction takes place. An Internet Intermediary is also designated as a "Platform," specifically including "social media operators, websites, blogs, media sharing websites, online discussion forums, streaming Platform, and other similarly oriented intermediaries" where user interaction takes place. Here, we see that no wording is used to describe the jurisdictional limit of the Code. The implication is that the Code is expected to have jurisdictional validity to platforms, small or large, whether or not they are based in Nigeria.

5.5. Large Service Platforms

Part III contains information on Large Service Platforms (LSPs)—"Interactive Computer Service Platform/Intermediary whose registered Users in Nigeria are more than 1 million" (NITDA Code, Definition). LSPs are to be incorporated in Nigeria (NITDA Code, Part III, § 1), have a physical contact address in Nigeria (NITDA Code, Part III, § 2), appoint a liaison officer for communication between the government and the platform (NITDA Code, Part III, § 3), provide human supervision to check the use of automated tools to strengthen accuracy, checkmate bias, ensure freedom of expression, and privacy (NITDA Code, Part III § 4), and provide information to users regarding why they receive certain adverts on their timelines (NITDA Code, Part III, § 5).

Going by the specification of over 1 million users for LSPs, it is clear that some local platforms qualify. For instance, there are popular blogs like "Linda Ikeji" with 7.4 million visits as of January 2024 (see SimilarWeb, 2024 https://www.similarweb.com/website/lindaikejisblog.com/#overview) and the discussion forum "Nairaland," which has more than 3 million members as of October 2024 (see https://www.nairaland.com/). LSPs also include global platforms such as Meta, Google, and X, showing that the Code applies to platforms, whether local or international. We also see NITDA's intention for platforms to have offices and be incorporated in Nigeria (and presumably pay corporate taxes in Nigeria). This implies an attempt to extend Nigeria's influence onto digital platforms, wherever they may be headquartered, as long as they have users in Nigeria. But given the balance of power realities (Takhshid, 2022), the indication is that these additional requirements for LSPs will likely be unenforceable. We only have to consider the aftermath of the X ban in 2021, where Nigeria signed an agreement with X before the ban was lifted. The first point of the agreement was for X to establish an office or "legal entity" in Nigeria within the first half of 2022 (see Okafor, 2022 https://www.premiumtimesng.com/news/headlines/505531-nigeria-lifts-twitter-suspension-after-seven-months.html?tztc=1). But X did not comply, and nothing has come by way of repercussions, pointing to balance of power realities.

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

The requirements and demands placed on LSPs can also apply to platforms that have less than 1 million users. This is because NITDA can designate a platform having less than 1 million users as large, "where it becomes necessary to preserve the sovereignty, security, public order, foreign diplomatic relations, and integrity of Nigeria" (NITDA Code, Part III, § 6). But again, we see the ambiguity, since the Code does not determine or provide examples of what qualifies under this clause. The determination rests with NITDA.

5.6. Information gathering

The discussion above has considered the standards set out in the Code, one of which is that platforms are required to moderate harmful or unlawful content, respectively, by carrying out risk assessments or executing removals within a reasonable period. How then can NITDA know whether platforms are responding to moderation requests? This is where information gathering comes in. It is a mechanism that makes it possible for regulators to monitor compliance and to know when a stipulation has been flouted (Lodge and Wegrich, 2012). In the Code, there is no provision for what users and other stakeholders can do if platforms do not respond to moderation notices. For instance, there is nothing that says users can report platform non-compliance to NITDA (or any other regulatory authority), a provision that could have served as an information-gathering mechanism for NITDA. NITDA itself is not expected to carry out information gathering on its own.

What the Code instead outlines is that platforms are expected to file annual compliance reports with NITDA (NITDA Code, Part II, § 10). The compliance report is to contain information on content moderation activities such as the number of complaints registered with a platform, the number of removed content with or without notices, and information on how children and adults are protected from harmful content.

This implies that the Code designates platforms as information providers, who carry out self-reporting. It means platforms are to report on their own compliance, with no provision on how the credibility of compliance reports will be assessed. It is effectively an admission by NITDA that it perhaps lacks the capacity to monitor platform compliance any other way. The Code also says nothing about how to handle cases where platforms fail to submit annual compliance reports. This suggests an underlying mindset (if not naivety) in NITDA—one where regulators expect, almost in a taken-for-granted manner, that platforms will comply with the Code. This underscores the challenges of enforcement that NITDA faces.

5.7. Broad application and weak enforcement

When it comes to enforcement, platforms are expected to take down content after complaints by users or government agencies. This means platforms are to "provide a dedicated channel" that authorised government agencies can use to send requests or complaints regarding unlawful or harmful content (NITDA Code, Part I, § 8). Platforms are also to provide a "complaint resolution mechanism for users to lodge complaints" (NITDA Code, Part I, § 9). Users can also ask for reviews or appeals (NITDA Code, Part I, § 10). From all indications, platforms have not complied with this stipulation to provide complaint resolution mechanisms for users. However, there are signs that government agencies are engaging with platforms like Google and TikTok (Apanpa, 2023), although there is nothing to suggest that platforms have provided dedicated channels that government bodies can use to lodge complaints.

In relation to the specifications of LSPs, there is some semblance to similar platform classifications in the EU's DSA. The DSA designates the biggest platforms as Very Lage Online Platforms and Very Large Online Search Engines—these are entities that have 45 million or more users in Europe (DSA, Article 33). They also have additional responsibilities such as providing annual transparency reporting obligations (DSA, Article 42), which is similar to the annual compliance reports that the NITDA Code requires from platforms. The difference, however, is that, unlike the European Commission, NITDA does not enjoy the balance of power symmetry to enforce co-regulatory mechanisms, whether in terms of mandating regular and accurate compliance reports or compelling the biggest platforms to comply—pointing to weak enforcement of the Code.

Beyond the balance of power concerns, other factors that account for weak enforcement of the Code include the vagueness, complexity, and broad application of its enforcement provisions. For instance, Part

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

IV of the Code deals with prohibited online materials that platforms are expected to remove. It defines prohibited materials as content that a court has declared to be so or is otherwise prohibited by 10 other laws, including the Cybercrimes Act 2015. This number of applicable external laws points to the broad scope that the Code entertains, a reality which could make enforcement not only confusing but also impractical.

Additionally, Part VI of the Code notes that non-compliance will mean a breach of three external laws: The Nigerian Communications Act 2003, the National Broadcasting Act 2004, and the NITDA Act 2007—the law that established NITDA. This implies that enforcement of platform non-compliance will be based on penalties in these laws, each of which has its respective enforcement stipulations—pointing to how vague and confusing enforcement of the NITDA Code is. For instance, in the Nigerian Communications Act 2003, if an organisation transgresses its provisions, the ranking officer of that organisation can be charged to court, with penalties of fines or imprisonment if found guilty (Nigerian Communications Act, § 139 & § 140). The NITDA Act 2007 contains a similar provision regarding fines and/or imprisonment for the ranking officer of a defaulting organisation (NITDA Act, § 17 & § 18). However, these provisions on imprisonment contravene the Code, which says "nothing in this Code shall impose criminal liability on an individual or individuals representing the Platforms" (NITDA Code, Part VI, § 3). For the National Broadcasting Act 2004, the main enforcement mechanism is the imposition of licence suspension (National Broadcasting Act, Third Schedule, Paragraph 9) or revocation (National Broadcasting Act, Third Schedule, Paragraph 8) on grounds such as violating the terms of the licence or acting contrary to the national interest. If the NBC Act is applied to social media as the Code presupposes, then it means platforms can be banned or stopped from operating in Nigeria—something on which the Code itself is silent.

By subjecting enforcement of the Code to provisions in external laws, therefore, NITDA has effectively made the Code complicating at best and most likely unenforceable, further weakening Nigeria's balance of power standing in the co-regulatory turn towards regulating social media platforms.

6. Discussion and conclusion

This article has highlighted the content of Nigeria's NITDA Code of Practice and its significance as a social media co-regulatory instrument in an African setting. The analysis was informed by a discussion of the prior regulatory trend in Nigeria and the balance of power realities that find expression when Global South countries attempt to regulate major tech platforms based in the Global North. Having presented all these, I now consider some implications. The first implication relates to the overarching design and content of the Code. It is important to note that the Code is not an Act of the National Assembly. Consequently, NITDA possibly opted for co-regulation because it has more of a technical remit unlike the National Assembly, which is more political and has an interest in directly influencing user discourse in online spaces (Olukolu et al., 2019). It could also be that NITDA, by adopting a co-regulatory turn, is imitating European policies (such as the DSA)—a possibility that highlights problematic and neo-colonialist thinking on the part of African policymakers, who tend to view European policies in superior terms as standards to replicate (Ayalew, 2023)—with the consequence being that unique policy solutions that are attuned to realities on the continent are sidelined. Or it could also be that NITDA has seen that direct user regulation, as represented by the 2015 Cybercrimes Act and the draft 2019 Internet Falsehood Bill, is simply unworkable (Obia, 2023a).

Whatever the case may be, the indication is that the Code, although a departure from direct user regulation, still contains elements of vagueness, complexity, and broad application, particularly when it comes to enforcement, as I touched on in the study findings. This leaves some sections of the Code open to interpretation, meaning it can become a tool of platform censorship and one that limits people's freedom of expression. The Code also contains a disproportionate focus on unlawful material compared to harmful content. This is understandable if we consider that unlawful materials are easier to deal with than harmful content—which are harder to pinpoint because they are "awful but lawful" (Errington, 2022, para 8). What is more consequential, however, is the disproportionate focus on mis/disinformation as opposed to other harms such as cyberbullying, doxing, or hate speech. This focus carries forward the emphasis that

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

we find in the draft Internet Falsehood Bill and, to some extent, the Cybercrimes Act. It, therefore, potentially limits NITDA's ability to address problematic online content as comprehensively as is required.

The second implication points to the faith that NITDA places in platform altruism—what can be said to be naïve faith since platforms almost always act in line with their profit motives (Klonick, 2018). Hence, NITDA's expectation that platforms should be involved, to a significant extent, in online harms research and media literacy funding requires critical evaluation. Although some platforms already fund research and media literacy activities in Nigeria, by giving platforms this mandate in an official manner without checks, NITDA shows that it is too trusting of platforms. What might work is for NITDA to request that platforms contribute to a trust, which can be administered jointly, with adequate controls, to support research and media literacy initiatives. Furthermore, the fact the Code does not provide for a system through which NITDA can carry out its independent investigation on platform compliance points to a limitation in the regulation. To address this, NITDA could have included a stipulation in the Code, where platforms are mandated to provide the Agency with full access to data on moderation requests and platform responses, including information on how platforms are protecting users from harmful content. To make this work, the stipulation would require platforms to institute a mechanism that flags moderation requests and platform responses with NITDA in real time. That way, the Agency will be able to monitor platform compliance based on trusted source data. But for this suggestion to materialise, NITDA would have to assess the powers of enforcement that it possesses.

What is therefore central to the discussion in this article is the power asymmetry that NITDA is confronted with in trying to enforce the Code—this is the third implication. Since its enactment in September 2022, there is no evidence that the Code has been enforced at any time or that platforms have submitted annual reports. To confirm, I examined the news and press release page on the NITDA website (see https://nitda.gov.ng/category/nitda-news/) in October 2024; the page contains information on NITDA's activities including enforcement. I found nothing on enforcement of the NITDA Code. I also sent an email to the NITDA information office on 22 December 2023 to ask for news on the enforcement of the Code, but there was no response. Overall, there is every reason to suggest that NITDA may only be able to enforce the Code on local websites and platforms (e.g., Nairaland), where the agency has a positive balance of power. When it comes to foreign LSPs where transborder application applies, we find a balance of power shortfall that presupposes that NITDA cannot carry out strict enforcement. In this regard, the example of X's non-compliance in the agreement it signed with Nigeria is telling. What complicates matters further is that the Code does not contain sanctions for platforms that default. Instead, sanctions are to be inferred from conflicting stipulations in other laws such as the Nigerian Communications Act—a reality that most likely makes the Code unenforceable and, therefore, toothless.

Similar challenges around power asymmetries also plague other African and Global South countries (Takhshid, 2022). This explains why many of them find it easier to target users and internet service providers that are locally based (Obia, 2023a). It also underscores why Global South countries prefer to use strategic internet blocking or social media bans: they serve as an effective, although anti-democratic, means for these countries to hold Big Tech platforms accountable (Common, 2023). One might, therefore, suggest that one way for countries like Nigeria to rebalance the power asymmetry is for them to democratise platform bans (temporary or permanent) by adding them as a means of last resort in legally compliant co-regulatory policies that are based on stakeholder views—ensuring that these bans meet the tests of necessity and proportionality. We see the United States, for instance, enacting legislation to ban TikTok on data security grounds if its Chinese owner does not sell it (see BBC, 2024 https://www.bbc.co.uk/newsround/68887270). But the balance of power concerns are again evident: the United States occupies the advantageous end of the scale as a Global North country, able to at least force negotiations at the highest levels in TikTok. It is almost inconceivable for a country like Nigeria to exert a similar level of influence, and fears that such a policy would be abused by the Nigerian political class for selfish purposes are valid. And if Nigeria succeeds in developing such a policy, there is nothing to say platforms will not deploy their political and economic might (e.g., lobbying policymakers or de-investing in Nigeria) to make it redundant. A co-regulatory policy that forces platforms to act would also mean they have to develop separate rules for

https://doi.org/10.1017/dap.2025.1 Published online by Cambridge University Press

Nigerian users, which raises questions about the Balkanisation of digital offerings and platform governance. These are hypothetical scenarios but underpinning them is the balance of power deficit, which, as I have argued in this article, demonstrates why it is difficult, and perhaps impracticable, for countries like Nigeria to enforce a co-regulatory regime on digital platforms based in the Global North.

Data availability statement. All resources used are included in the text and references. Where they are available online, a link is provided.

Author contribution. The author was solely responsible for conceptualisation, formal analysis, investigation, methodology, project administration, writing the original draft, and reviewing and editing the revised draft.

Funding statement. This work received no specific grant from any funding agency, commercial, or not-for-profit sectors. For the purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising. Open access funding was provided under the University of Sheffield Institutional Open Access Fund.

Competing interest. The author declares no competing interests.

References

Abdullateef M (2021) Regulating social media in Nigeria: A quantitative perception study. *Political Science 2*(1), 52–77. Available at https://www.researchgate.net/profile/Mohammed-Abdullateef/publication/346717844_Regulating_social_media_in_Nigeria_A_quantitative_perception_study/links/617bb2283c987366c3fc48ff/Regulating-social-media-in-Nigeria-A-quantitative-perception-study.pdf.

Apanpa O (2023) Social media regulation: We are engaging Google, TikTok, says NBC. *Punch*, 13 October 2023. Available at https://punchng.com/social-media-regulation-we-are-engaging-google-tiktok-says-nbc/.

Ayalew Y (2023) The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. Available at https://www.ejiltalk.org (accessed 23 September 2022).

Balkin J (2018) Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UC Davis Law Review 51*(1149), 1149–1210. Available at https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-3_Balkin.pdf.

Bizberge A, **Mastrini G and Gómez R** (2023) Discussing internet platform policy and regulation in Latin America. *Journal of Digital Media & Policy 14*(2), 135–148.

Bradshaw S, **Bailey H and Howard P** (2020) Industrialized disinformation: 2020 global inventory of organized social media manipulation. Available at https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20-FINALv.3.pdf (accessed 12 January 2020).

BBC. (2024). TikTok: Joe Biden approves law that could ban the app in America. https://www.bbc.co.uk/newsround/68887270 (Accessed 3 October 2024).

Carter E (2017) Mass communication law and policy research and the values of free expression. *Journalism & Mass Communication Quarterly 94*(3), 641–662. https://doi.org/10.1177/1077699017717694.

Chari T (2022) Between state interests and citizen digital rights: Making sense of internet shutdowns in Zimbabwe. In Kperogi F (ed.), *Digital Dissidence and Social Media Censorship in Africa*. London: Routledge, pp. 76–97.

Coleman D (2019) The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law 24*, 417–439.

Common M (2023) Beyond the usual suspects: A taxonomy of social media regulations in countries with human rights issues. *International Review of Law, Computers & Technology 37*(1), 1–28. https://doi.org/10.1080/13600869.2022.2043093.

De Gregorio G and Stremlau N (2021) Platform governance at the periphery: Moderation, shutdowns and intervention. In Bayer J, Holznagel B, Korpisaari P and Woods L (eds), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance across the Globe*. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co., pp. 433–450.

DeNardis L and Hackl A (2015) Internet governance by social media platforms. *Telecommunications Policy 39*, 761–770. https://doi.org/10.1016/j.telpol.2015.04.003.

Edwards L, **Obia V**, **Goodman E and Spasenoska S** (2023) Cross-sectoral challenges to media literacy. Available at https://www.gov.uk/government/publications/cross-sectoral-challenges-to-media-literacy (accessed 12 December 2023).

Elega A, **Mohammed A and Oloyede F** (2023) "The fall of a dry leaf is a warning to the green ones": Exploring the twitter ban and the impending dangers of data politics, algorithmic governance, and mass surveillance in Nigeria. *First Monday 28*(4), 1–15. https://doi.org/10.5210/fm.v28i4.12692.

Errington K (2022) Lawful but awful: What to do about harmful online content? Available at https://helenclark.foundation/publications-and-medias/lawful-but-awful-what-to-do-about-harmful-online-content/ (accessed 13 January 2024).

Fombad C (2022) Democracy and fake news in Africa. *Journal of International and Comparative Law 9*(1), 131–154. Available at https://www.jicl.org.uk/journal/june-2022/democracy-and-fake-news-in-africa.

Fuchs C and Sandoval M (2015) The political economy of capitalist and alternative social media. In Atton C (ed.), *The Routledge Companion to Alternative and Community Media*. London: Routledge, pp. 165–175.

Garbe L, **Selvik L and Lemaire P** (2021) How African countries respond to fake news and hate speech. *Information, Communication & Society 26*(1), 86–103. https://doi.org/10.1080/1369118X.2021.1994623.

Gerbaudo P (2013) The "kill switch" as "suicide switch": Mobilising side effects of Mubarak's communication blackout. *Westminster Papers in Communication and Culture 9*(2), 25–46. https://doi.org/10.16997/wpcc.165.

Gumede W (2016) Rise in censorship of the internet and social media in Africa. *Journal of African Media Studies 8*(3), 413–421. https://doi.org/10.1386/jams.8.3.413_7.

Hardy J (2014) *Critical Political Economy of the Media: An Introduction*. Abingdon, Oxon: Routledge.

Kalemera A, **Kapiyo V**, **Kimumwe P**, **Nalwoga L**, **Nankufa J**, **Wanyama E and Wakabi W** (2020) State of internet freedom in Chad 2019: Mapping trends in government internet controls, 1999–2019. *CIPESA*. Available at https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Chad-2019.pdf (accessed 8 May 2021).

Kaye D (2019) *Speech Police: The Global Struggle to Govern the Internet*. New York: Columbia Global Reports.

Klonick K (2018) The new governors: The people, rules, and processes governing online speech. *Harvard Law Review 131*, 1598–1670. Available at https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf.

Kwet M (2019) Digital colonialism: US empire and the new imperialism in the global south. *Race & Class 60*(4), 2–26.

Lodge M and Wegrich K (2012) *Managing Regulation: Regulatory Analysis, Politics and Policy*. London: Bloomsbury Publishing.

Lunt P and Livingstone S (2012) *Media Regulation: Governance and the Interests of Citizens and Consumers*. London: Sage.

Manganelli A and Nicita A (2022) *Regulating Digital Markets: The European Approach*. Chan, Switzerland: Palgrave Macmillan.

Marchant E and Stremlau N (2019) Africa's internet shutdowns: A report on the Johannesburg Workshop. Available at https://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2019/10/Internet-Shutdown-Workshop-Report-171019.pdf (accessed 23 April 2023).

Marsden C and Meyer T (2019) How can the law regulate removal of fake news? Available at https://www.scl.org/articles/10425-how-can-the-law-regulate-removal-of-fake-news (accessed 14 October 2021).

Moses J, **Targema T and Ishaku J** (2022) Tale of an ill-fated scapegoat: National security and the struggle for state regulation of social media in Nigeria. *Journal of Digital Media & Policy*, *15*(1), 27–45. https://doi.org/10.1386/jdmp_00100_1.

Nakaayi A (2022) Case studies on anti-social media laws in African countries. In Kperogi F (ed.), *Digital Dissidence and Social Media Censorship in Africa*. London: Routledge, pp. 242–266.

Nyabola N (2023) Seeing the forest—and the trees: The global challenge of regulating social media for democracy. *South African Journal of International Affairs 30*(3), 455–471. https://doi.org/10.1080/10220461.2023.2270461.

NITDA Code. (2022). Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries. https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf

Obia V (2021) Are social media users publishers? Alternative regulation of social media in selected African countries. *Makings 2*(1), 1–13. Available at https://makingsjournal.com/wp-content/uploads/2021/08/Vincent-Obia-2021.pdf.

Obia V (2023a) Regulatory annexation: Extending broadcast media regulation to social media and internet content. *Communication Law and Policy 28*(2), 99–123. https://doi.org/10.1080/10811680.2023.2206382.

Obia V (2023b) *Regulatory annexation and the matrix of dependence: The regulation of social media in Nigeria*. PhD dissertation, School of Media, Birmingham City University.

Olukolu R, **Ogwezzy-Ndisika A**, **Faustino B and Oloruntoba F** (2019) Social media regulation and challenges of communication in an evolving Nigerian society. *University of Baltimore Journal of Media Law and Ethics 7*(1–2), 68–84.

Okafor, C. (2022). Updated: Nigeria lifts Twitter suspension after seven months. Premium Times. https://www.premiumtimesng.com/news/headlines/505531-nigeria-lifts-twitter-suspension-after-seven-months.html?tztc=1 (Accessed 14 January 2024).

Obia, V. (2020). #EndSARS, a unique Twittersphere and social media regulation in Nigeria. https://blogs.lse.ac.uk/medialse/2020/11/11/endsars-a-unique-twittersphere-and-social-media-regulation-in-nigeria/ (accessed 11 November 2020).

Paradigm Initiative. (2022). An open call to NITDA to review the updated Code of Practice. https://paradigmhq.org/an-open-call-to-nitda-to-review-the-updated-code-of-practice/ (Accessed 29 September 2023).

Rukundo S (2018) "My president is a pair of buttocks": The limits of online freedom of expression in Uganda. *International Journal of Law and Information Technology 26*(3), 252–271. https://doi.org/10.1093/ijlit/eay009.

SimilarWeb. (2024). Linkaikejisblog website analysis for 2024. https://www.similarweb.com/website/lindaikejisblog.com/#overview (Accessed 30 September 2024).

Takhshid Z (2022) Regulating social media in the global south. *Vanderbilt Journal of Entertainment & Technology Law 24*(1), 1–57. Available at https://scholarship.law.vanderbilt.edu/jetlaw/vol24/iss1/1/.

Vareba A, **Nwinaene V and Theophilus S** (2017) Internet censorship and freedom of expression in Nigeria. *International Journal of Media Journalism and Mass Communication 3*(2), 25–30. Available at https://www.arcjournals.org/pdfs/ijmjmc/v3-i2/4.pdf.

Wagner B (2018) Understanding internet shutdowns: A case study from Pakistan. *International Journal of Communication 12*, 3917–3938. Available at https://ijoc.org/index.php/ijoc/article/view/8545.

Cite this article: Obia V (2025). Digital policy and Nigeria's Platform Code of Practice: towards a radical co-regulatory turn. *Data & Policy*, 7: e12. doi:10.1017/dap.2025.1