CIVIL SOCIETY COALITION MEMO TO THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA) ON THE DRAFT CODE OF PRACTICE FOR INTERACTIVE COMPUTER SERVICE PLATFORMS/INTERNET INTERMEDIARIES

JUNE 24, 2022

SECTION 1:INTRODUCTION

The advancement of digital technology has brought with it attendant concerns. Platform usage has soared among citizens of various countries. Thus, with more users accessing these platforms, more content is produced and consumed than at any other point in history. Consequently, recent years have seen a growth in the clamour for content moderation online. Indeed, governments, interactive computer service platforms and internet intermediaries have grappled with how to moderate what is deemed harmful content. The attempts to straddle the tension and ability to keep users safe, protect their data and privacy, and prevent government overreach, have become apparent.

Although co-moderation is necessary, systems must not rush to create simple solutions to complex problems while risking human rights rightfully protected by the Nigerian constitution, regional instruments & international law. Any attempt to moderate digital spaces without consultations with relevant stakeholders, including platform owners, civil society actors and users, presents the risk of human rights abuses, including infringing on the rights of freedom of expression and privacy & can lead to censorship.

Laws and regulations must centre on the people and their human rights. This human-centric approach gives credence to the democratic law-making process where all citizens, regardless of class and status, are duly represented. It also preserves their rights to provide input to the laws, thus legitimising the system as one that serves the people. This process is what the letter of The Rule Making Process Regulation of NITDA attempts to establish. The process must be transparent and evident during the lawmaking process and not after the fact. It is unacceptable to have clandestine rulemaking processes foisted upon citizens while, in the process, their voices are silenced. Transparency is necessary for internet governance and must factor in the crucial function of multi-stakeholder governance.

This draft code of practice represents an opportunity to protect the digital rights of Nigerians online. Still, it should not be used in the same vein to stifle, harass and unlawfully surveil citizens and users. It is also unacceptable to include provisions within this code of practice that circumvent previous provisions established in the Constitution. It further circumvents powers allotted to other relevant agencies such as the National Agency for the Prohibition of Trafficking in Persons (NAPTIP), Independent Corrupt Practices Commission (ICPC), and Economic and Financial Crimes Commission (EFCC), amongst others. It is imperative then that any such code or attempt at regulating Nigeria's digital space must be carried out in good faith.

SECTION 2:GENERAL INPUT ON CODE OF PRACTICE

As a coalition of organisations committed to the preservation of the digital rights and safety of all those existing within Nigeria, we recommend that the following amendments be made to this draft code of practice:

a. **Contradictory Stipulations:** The code has contradictory stipulations, e.g. Part I on RESPONSIBILITIES OF INTERACTIVE COMPUTER SERVICE PLATFORMS/INTERNET INTERMEDIARIES stipulates content flagged as illegal within 24 hours — yet Part II asks that verifications first be made.

b. **Address Multistakeholderism**: Internet governance covers a wide range of stakeholders, which include children, minority groups, academics, journalists and content creators, businesses as well as various government organisations. These multiple stakeholders need to be visibly involved in the internet governance process, from consultation to certain levels of decision-making and implementation. Considerations should include a governance board with these stakeholders represented adequately.

c. **Data Privacy**: Part II on ADDITIONAL RESPONSIBILITIES provides that data be stored, including information that has been deleted or flagged by the government. No mention was made of how long such data can be held. Indefinite access to user data that is no longer available to the user contravenes the right to be forgotten in the NDPR and breaches the right to privacy. NITDA, the enforcer of the regulation, raises concerns about the ability of the agency to provide oversight over itself.

d. **Oversight Functions:** Constitutionally, Nigeria ensures that no arm of government is left to its whims, and although court orders are mentioned in Part I mainly, there are no further stipulations for supervisory functions over NITDA, especially as there are no additional instances of oversight relating to Point 5.

e. **Reports:** Transparency reports are released to the public by the private sector based on accountability, which should be modelled on reporting mechanisms made by interactive computer service platforms/internet intermediaries. The government should also commit to transparency around the disclosure of requests. These should include the details of the government's (both state

and federal) requests for action posts and accounts. The obligation should be fulfilled through the publication of a transparency report publicly that will highlight the number and nature of requests from the government.

f. **Citizen Awareness/Enlightenment:** Agency focus should be directed toward educating and empowering citizens on their rights alongside ways to protect themselves online. It should also encompass government efforts to protect them through reporting pipelines with law enforcement and the courts. The agency should seek to enlighten the public on appropriate channels via which complaints can be submitted in instances of infringing digital rights.

g. **Vague Stipulations:** The code attempts to address various offences of different natures and burdens of proof within a single line. These stipulations are far too ambiguous in contrast to other pieces of legislation which have already taken time to define relevant terms painstakingly. For instance, Point 2 of Part II requires platforms to:
"...inform users not to create, publish, promote, modify, transmit, store or share any content or information that is defamatory, libellous, pornographic, revenge porn, bullying, harassing, obscene, encouraging money laundering, exploiting a child, fraud, violence, or inconsistent with Nigeria's laws and public order".

This line covered offences already outlined in the Violence Against Persons (Prohibition) Act, Administration of Criminal Justice Act, CyberCrime (Prohibition, Prevention, etc.) Act, Child Rights Act, Money Laundering Act, and more.

h. **Existing Legislative Efforts**: The agency should focus on supporting the passing of relevant legislation such as the Digital Rights and Freedoms Bill and the Data Protection Bill.

SECTION 3: RECOMMENDATIONS

OBJECTIVES

a. "*Set out best practices required of Interactive Computer Service Platforms/Internet Intermediaries*."

The agency does not have the statutory mandate to undertake this function.

b. "*Set out best practices that will make the digital ecosystem safer for Nigerians and non-Nigerians in Nigeria."*

The digital ecosystem is broad, and thus a scope needs to be better defined to ensure that no one agency goes ultra vires.

c. *"Set out measures to combat online harms such as disinformation and misinformation."*

Information and communication are already housed within the mandate of the NCC, NBC and Ministry of Information and Culture.

d. *"Adopt and apply a co-regulatory approach towards implementation and compliance."*

The code barely refers to other stakeholders as "co-regulators"; it continues to list NITDA as the singular regulatory agency.

DEFINITION

The Code of Practice does not explain some key terminology thoroughly within the various contexts they appear as listed throughout this document.

Part I: RESPONSIBILITIES OF INTERACTIVE COMPUTER SERVICE PLATFORMS/INTERNET INTERMEDIARIES

a. **Point 1:** *"Abide by Nigerian laws and not deploy or modify their Platform in any way that will undermine or interfere with the application and/or enforcement of the law."*

What qualifies deployment or modifications against the government is unclear and vague. The template ought to use a template that explains such deployment and modifications for these platforms. Such a part has a bearing on encryption bearing in mind the very nature of platforms

such as Whatsapp with end-to-end encryption in place to ensure the privacy of personal communications. The vagueness of this section does not shed light on what is legitimate and may unreasonably go towards regulating the very design of platforms and be used arbitrarily to censor expression.

b. **Point 3: "***Act expeditiously upon receiving a notice from a user, or an authorised government agency of the presence of an unlawful content on its Platform. A Platform must acknowledge the receipt of the complaint and take down the content within 24 hours."*

Suppose just "a user" reports content and platforms are directed to take down content because he/she deems it unlawful. In that case, this has the potential to trample on the human rights of others, especially if multiple users have not reported this content. This Part leaves no room for safeguards to fundamental rights, particularly freedom of expression and access to information. Principle 39(4) and (5) of the ACHPR Declaration of Freedom of Expression and Access to Information clearly states as follows, which must be instructive:

4. States shall not require the removal of online content by internet intermediaries unless such requests are:

a. clear and unambiguous;
b. imposed by an independent and impartial judicial authority, subject to sub-principle 5;
c. subject to due process safeguards;
d. justifiable and compatible with international human rights law and standards; and
e. implemented through a transparent process that allows a right of appeal.

5. Law-enforcement agencies may request intermediaries for the expedited or immediate removal of online content that poses an imminent danger or constitutes a real risk of death or serious harm to a person or child, provided such removal is subject to review by judicial authority

c. **Point 5: "***Disclose the identity of the creator of information on its Platform when directed to do so by a Court order. Provided that an order of this nature shall apply for the purpose of preventing, detecting, investigating, or prosecuting an offence concerning the sovereignty and integrity of Nigeria, public order, security, diplomatic relationships, felony, incitement of an offence relating to any of the above or in relation to rape, child abuse, or sexually explicit material. Where the first creator of the message in question is located outside Nigeria, the first creator of that information in Nigeria shall be deemed to be the first creator***. ***Where the first***

creator of the message in question is located outside Nigeria, the first creator of that information in Nigeria shall be deemed to be the first creator."

Something already in creation cannot be "created" again. Such a provision leaves the interpretation to "reposting", "sharing", "retweeting", "liking", etc. Enforcing these actions on the creators of content that did not originate from within the country and tagging them as its first creator creates unnecessary & unfair responsibility.

d. **Point 6:** *Exercise due diligence to ensure that no unlawful content is uploaded to their Platform. Where a Platform receives a notice from a user or any authorised government agency that an unlawful content has been uploaded, such Platform is required to take it down and ensure it stays down. No liability shall be incurred by a Platform where such Platform has taken all reasonable steps to ensure that an unlawful content is taken or stays down.*

   In instances where circumstances around what is deemed "unlawful content" are contestable, platforms should be able to launch an independent investigation, especially if it defies standard global protocols on the protection of digital rights and extension of fundamental human rights. Consideration should be made for a room to appeal and resolve such contention.

e. **Point 11:** *Make provision for verifying official government accounts and authorised government agencies subject to approval by NITDA. The account shall only be used for official purposes and NITDA reserves the right to withdraw approval by notifying the Platform in writing, stating the grounds for such action.*

   The verification process pathway for government agencies going through NITDA is problematic. Platforms should reserve the right to verify government agencies on their platform subject to the application filled out by the specific government agency. NITDA serving as the middle man is completely redundant given that there is already a standard procedure for platform verification.

Part II: ADDITIONAL RESPONSIBILITIES

3. *Carry out risk assessment to determine whether a content is harmful, upon receiving a notice. A Platform shall take steps to mitigate and manage the impact of such content and ensure that the community rules or guidelines specify how children and adults will be protected from harmful content*

which they may encounter. In assessing such content, a Platform shall consider: a) The nature of the content, and if there is a material risk of it having a direct or indirect physical or psychological impact on a child or an adult. b) That there is a material risk of the content's dissemination having a physical or psychological impact on a child or an adult. Consideration should be given to: i. The level of risk or harm posed by the content; ii. The potential reach and interaction with the content c) The socio-cultural peculiarities of Nigeria.

This contradicts the initial request for 24-hour feedback. It also brings the question of who determines content is harmful? Government, an established law, or platform. In addition, the provision fails to provide the timeline to complete a risk assessment. We recommend the clarification of the provision for inconsistency with other provisions of the Code.

"Online Harm" is broadly defined as "any action with a reasonably foreseeable risk of having negative physical or psychological effects on individuals." As such, the language used in defining harmful content in the document is hazy.

Also, responding 24 hours after receiving a request seems unrealistic. Before making a choice or completing a transaction, a company must do due diligence in order to protect itself from being held accountable for any misuse or damage caused by releasing this data to the government agency. This involves a series of processes required by standards; how is that realistic, considering that some laws in other jurisdictions allow up to 72 hours to carry out proper due diligence. In short, the 24-hour time limit for the removal of unlawful content usually results in erroneous and forced takedowns of legitimate content, which may lead to censorship.

What and who defines the socio-cultural peculiarities of Nigeria? This is another instance where a group of designated people with oversight should ensure all interests are covered.

6. *Preserve any information concerning a person that is no longer a user of a Platform due to withdrawal or termination of registration, or for any other reason, as required by law.*

When personal data has served its purpose, or the data subject no longer consents to the collection or storage of personal data, the data subject has the right under the NDPR to prevent or restrict the further disclosure of or processing of personal data. This appears to be in conflict with an NDPR clause of the right to be forgotten. This also suggests a traceability option.

9. *File an annual compliance report with NITDA that indicates the: a) Number of registered users on its Platform in Nigeria; b) Number of active registered users on its Platform in Nigeria; c) Number of closed and deactivated accounts in Nigeria; 8 d) Number of removed content with and without notice or Court order; e) Number of contents put back with or without notice; f) Number of contents removed and reuploaded; g) Information on how children and adults are protected from harmful content which they may encounter; h) Information on the number of complaints registered with a Platform; i) Number of resolved and unresolved complaints; j) Independent awareness report on disinformation and misinformation; k) Number of contents taken down due to disinformation and misinformation; l) Any other relevant information.*

Why NITDA and not a public report, especially for transparency? Why not other information and identity agencies? In the face of enacting such restrictions, NITDA has not offered a means to combine or balance the interests of many stakeholders. What procedures are in place to involve other parties who might be interested in the report? The security agencies, as an example. Additionally, the clause downplays the relevance of business self-governance in terms of privacy and data protection.

In summary, there are many reasons to be concerned from the perspective of human rights, and it is troubling that the guidelines include almost no mention of human rights, especially the right to privacy and the freedom of expression (which is mentioned only once in passing in Part III). Particularly troubling is the haziness surrounding how the standards apply to encrypted connections.

Part III: LARGE SERVICE PLATFORMS

All Platforms whose users are more than one hundred thousand (Large Service Platform) shall, in addition to the responsibilities stated above:

It should be stated clearly if "100,000 users" refers to the total number of users on the platform or the number of Nigerian users on the platform.

Part IV: PROHIBITION

A platform shall not continue to keep prohibited materials or make them available for access when they are informed of such materials. Prohibited materials are those which is objectionable on the grounds of public interest, morality, order, security, peace or are otherwise prohibited by applicable Nigerian laws.

"Morality" - is also a word in need of definition as Nigeria is a multifaceted secular state whose morals differ according to socio-cultural realities.

The loophole here is that existing laws could be used to prosecute while these laws are problematic. This is the time to examine existing laws and see issues that violate human rights.

The definition of prohibited materials is overly broad and subject to subjective interpretation. The effect of this Part is that it limits freedom of expression online under subjective and excessively broad terms such as morality and public interest. The obvious outcome of this kind of provision is that it will not meet the test of legitimacy, necessity and proportionality. This is an explicit provision violating freedom of expression against the Constitution of Nigeria under section 39(1) and articles 9 and 19 of the African Charter on Human and Peoples' Rights and International Covenant on Civil and Political Rights. Morality is an ever-changing term across cultures in terms of Siracusa Guidelines.

A State invoking public morality as a ground for restricting human rights should demonstrate that the limitation in question is essential to maintaining respect for the fundamental values of the community. In the absence of adequate and meaningful consultations, which ideally are part of a lawmaking process, this cannot be said to be a reasonable limitation being imposed by this Part, moreso through a Code of Practice. In addition, Principle 23(3) of the ACHPR Declaration of Principles on Freedom of Expression and Access to Information stipulates that States shall not prohibit speech that merely lacks civility or which offends or disturbs. The same main principle outlines what should fall within the ambit of prohibited speech, and this Code does not bring such clarity.

Part V: MEASURES ON DISINFORMATION AND MISINFORMATION

a. The Code of Practice does not explain some key terminology thoroughly within the various contexts they appear as listed throughout this document. Points 1 - 10 do not clearly explain the terms under reference as no universally accepted definitions of Mis and Disinformation currently exist. In such cases, content providers and or citizens' rights may be infringed on account of government interest in any given issue, even if it's not for the public interest.

b. Terms such as "false" or" misleading" are not clearly defined. Is an item misleading because of intent or due to the effect? In the latter case, users who have been exposed to false information and unwittingly published such inadvertently become unduly implicated. They consequently become targets in the attempt to address incorrect information while the issue is not curbed in actuality.

c. Point 6: *"Engage the services of certified factcheckers to identify information targeted to disinform or misinform users in Nigeria."*

   This stipulation lacks adequate criteria to ascertain who is identified as a "certified fact-checker." This stipulation leaves room for malicious intent to be perpetrated.

d. Point 7a: *"A user shall not be liable, without intent, for merely redistributing through intermediaries, the content of which they are not the author and which they have not modified."* This point contradicts Part I on the user who shares and on whom the burden of responsibility rests. It also deems misinformation as not being harmful content.

e. Point 8: *"Provide users with easily accessible tools to report disinformation and/or misinformation and improve access to different authentic sources with alternative perspectives."*

   This stipulation is redundant as each digital platform currently contains reporting pathways and mechanisms. These channels also include label warnings to users for such content, with reports supplied after moderation of the flagged content is complete.

SECTION 4: SIGNATURES

Signed by

1. Paradigm Initiative
2. TechHerNG
3. Avocats Sans Frontières France.
4. Human Rights Journalists Network
5. Enough is Enough Nigeria
6. Impact Foundation For Youths Development
7. Afrika Youth Movement
8. Voice Of the Vulnerables
9. Tech Hive Advisory
10. Ikigai Innovation Initiative
11. Smith Nwokocha
12. International Press Institute (IPI)