OLANIWUN AJAYI

MAY 2025

Exposition of the Whitepaper on the Online Harms Protection Bill

OALP Technology Innovation and Fintech Newsletter

INTRODUCTION

Following Nigeria's first Content Moderation (**CM**) and Online Safety Summit,[1] the National Information Technology Development Agency (**NITDA**) in collaboration with the Advocacy for Policy and Innovation (**API**)[2] published a white paper on the framework for an Online Harms Protection (**OHP**) Bill in Nigeria (the **White Paper**).[3] The White Paper emphasises the prevalence of online harms and threats; proposes a shift from the current CM-centered approach towards a duty-of-care ethos, stakeholder partnership and a coordinated framework that guarantees citizens' rights while shielding society from the harms of the internet. The White Paper further analyses efforts by several jurisdictions in combating online harms, proposing strategies that are best suited for Nigerian peculiarities. With the White Paper, NITDA and API intend to spark a national dialogue on OHP,[4] which will shape and guide policy development in creating an effective legal framework on OHP and encourage stakeholder participation.

In this exposition of the White Paper, we examine the White Paper and proposed strategies for combating online harms in Nigeria. Consequently, we query the strengths, gaps, and the overall alignment of the framework with best practices in digital governance. Ultimately, we propose recommendations to the framework to effectively counter online harms in Nigeria, drawing guidance from relevant jurisdictions.

OVERVIEW OF THE WHITE PAPER

The White Paper identifies the challenges of online harms and the importance of CM while preserving digital rights. It also identifies the inadequacies of conventional CM practices and the lack of consistency and transparency of self-regulatory measures to address these practices, which often lead to accusations of bias and censorship. Furthermore, the White Paper highlights that automated systems of CM usually struggle with language and local nuances, which results in over- or under-moderation. It also notes that human moderators face a psychological toll while reviewing disturbing content.

The White Paper examines the pros and cons of both Artificial Intelligence (**AI**) moderation and human moderation and proposes a hybrid CM mechanism that combines the benefits of both AI and human moderation for effective and efficient CM practices and quality.

Further, the White Paper proposes a legal framework specifically for OHP that moves from the conventional CM approach to a proactive model of OHP. This framework emphasises citizen protection through a co-regulatory and "duty-of-care" model. The White Paper proposes an OHP Bill that focuses on a multi-stakeholder, participatory, and inclusive approach to address the challenges posed by online harm, safeguarding digital rights while reflecting Nigeria's unique digital realities.

1. *This Summit was held in July 2022.*
2. *API is an Africa-focused non-profit organisation dedicated to advancing digital innovation and inclusive policy development.*
3. *National Information Technology Development Agency (NITDA), Framework for Online Harms Protection in Nigeria (December 2024) (hereinafter the White Paper) https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf (accessed 20 January 2025).*
4. *Feedback, comments, and recommendations on the paper are to be provided via theOHPwhitepaper.secretariat@apiintelligence.org.*

Categorisation of Illegal Content and Harmful Content

The White Paper distinguishes between "illegal content" and "harmful content". Illegal content refers to material that violates existing laws, such as child sexual exploitation and abuse material, hate speech, terrorism-related content, and cyberstalking.[5] Harmful content, while not necessarily illegal, is content that has the potential to impact individuals or communities negatively. Examples include misinformation, disinformation, and extremist content that may provoke social or political unrest.[6] This categorisation ensures a nuanced approach, enabling tailored strategies for addressing each type of content.

The White Paper emphasises that while illegal content requires strict enforcement under the law, harmful content demands a more balanced approach to prevent infringements on the right to freedom of expression. This distinction informs the proposed duty-of-care model, and the responsibilities assigned to intermediaries and regulators.

Potential Impact of Algorithms

According to the White Paper, algorithms play a dual role in CM and shaping online interactions. On one hand, algorithms enable efficient CM at scale by swiftly flagging or removing harmful content.[7] They also power recommendation systems that enhance user engagement and accessibility to relevant content. On the other hand, due to their opacity and inherent biases, algorithms often exacerbate online harms.[8] For instance, algorithmic amplification can spread misinformation or promote polarising content, deepfakes, voice clones, and synthetic media, while biased moderation systems may disproportionately target marginalised groups.

The White Paper proposes that algorithms should be trained on diverse datasets that accurately represent the local user base.[9] This involves integrating cultural, linguistic, and demographic diversity into the training process.[10] The White Paper also proposes that while AI handles large-scale content screening, human moderators should be responsible for context-sensitive decisions; a collaborative approach combining AI and human judgment ensures nuanced moderation and minimises errors. In addition, algorithms should be periodically reviewed and audited to assess their impact on various demographics, improve accuracy and prevent biases or harmful outcomes.[11] Furthermore, CM algorithms should be fair, avoid disproportionately affecting marginalised communities, and incorporate oversight, appeals mechanisms and transparency to foster trust and enable external scrutiny.[12]

Content Moderation Practices: Human and AI Moderation

The White Paper examines current CM practices and identifies human moderation and AI-powered systems as critical tools for managing online harms.[13] Human moderation offers the advantage of contextual understanding, enabling nuanced decision-making in complex cases. However, it is resource-intensive and subject to human biases.[14]

AI-powered moderation, on the other hand, excels in processing vast amounts of content rapidly, identifying harmful patterns, and enforcing platform policies at scale.[15] Despite these advantages, AI systems are not infallible.[16] They often struggle with contextual nuances and may erroneously flag legitimate content as harmful or fail to detect subtle instances of harm.[17]

The White Paper calls for a hybrid approach that leverages the strengths of both human and AI moderation.[18] It also underscores the importance of training moderators, auditing AI systems, and incorporating user feedback to enhance the effectiveness and fairness of content moderation practices.[19]

Duty-of-Care

The White Paper postulates the introduction of a duty-of-care model based on lessons from Germany's Network Enforcement Law, EU's Digital Services Act, and Brazil's Fake News Bill.[20] It defines "duty of care" as the legal obligation placed on internet service providers, social media platforms, search engines, and online intermediaries to take reasonable measures to avoid harm to users from content transmitted or stored on their platforms. This will place a proactive responsibility on online platforms and

5. *The White Paper, p. 20.*
6. *Ibid.*
7. *The White Paper, pp. 24-25.*
8. *Ibid.*
9. *The White Paper, p. 27.*
10. *Ibid.*
11. *The White Paper, p. 28.*
12. *Ibid.*
13. *The White Paper, p 47.*
14. *The White Paper, pp. 47-48.*
15. *The White Paper, p. 48.*
16. *The White Paper, pp. 49-50.*
17. *Ibid.*
18. *The White Paper, p. 51.*
19. *Ibid.*
20. *The White Paper, p. 29.*

intermediaries to prevent, detect, and mitigate online harms. This model shifts the focus from reactive CM to preventive measures that prioritises user safety.

Under this model, platforms are required to conduct risk assessments to identify potential harms posed by their services and implement mitigation mechanisms. Examples include age-appropriate controls, user-friendly reporting systems or mechanisms to report harmful content and transparent CM policies.[21] The duty-of-care model also seeks to balance the harms prevention with the protection of users' rights, including freedom of expression and privacy.[22]

Co-regulatory Approach

The co-regulatory approach to CM is another key proposition of the White Paper. This approach proposes a combination of government oversight, stakeholders' involvement, and internet platforms participation to establish a balanced framework for addressing harmful content.[23] The co-regulatory model is designed to be flexible, inclusive, and adaptive, accommodating the evolving nature of online harms and digital technologies.

In practice, it is expected that this approach would involve platforms taking primary responsibility for implementing harm mitigation measures while being subject to oversight and guidance from regulatory authorities. Civil society organisations are critical in monitoring compliance, advocating for digital rights and providing feedback on the framework's effectiveness. This multi-stakeholder collaboration should enhance accountability and ensure diverse perspectives are represented in regulatory decisions.

Intermediary Liability

Intermediary liability addresses the legal responsibility of intermediaries, such as internet service providers, online platforms, search engines, web hosting companies, and content delivery networks, in moderating content and mitigating harms.[24] The proposed framework establishes obligations for intermediaries to act swiftly in removing illegal content once notified, while ensuring that these actions do not infringe on legitimate expression.[25] The proposed framework introduces safeguards to prevent overreach. For instance, it emphasises the need for

intermediaries to provide transparency in their moderation practices and to offer users the ability to contest content removal decisions.[26] By striking this balance, the proposed framework aims to promote accountability without stifling creativity or free expression.

End-to-End Encryption (E2EE)

The White Paper recognises end-to-end encryption (E2EE) as a critical tool for protecting user privacy and securing communications.[27] Many messaging platforms have adopted E2EE to secure the integrity and confidentiality of user-generated content and information.[28] However, encrypted communications pose challenges for OHP, as they are inaccessible to platforms and regulators.[29]

The White Paper highlights a striking concern: that while E2EE effectively shields legitimate users from unauthorised access and surveillance, it can also provide a clandestine cover for wrongdoers to engage in online harm, such as cyberbullying, harassment, hate speech or other malicious activities. At the same time, E2EE remains central to private communication and is fundamental to preserving freedom of expression and privacy.

The White Paper further expounds on the rationale for excluding E2EE from OHP as follows: (x) upholding freedom of expression, (y) protecting privacy and security, (z) technical and practical limitations of E2EE, (xx) international precedents, (yy) the risk of undermining trust, and (zz) balancing safety with rights.

Accordingly, the White Paper proposes an approach beyond policing-specific technology. The combination of encryption preservation, co-regulatory practices, and the imposition of a duty of care reflects a holistic strategy to address the complexities of online safety in the digital landscape.

21. *Ibid.*
22. *Ibid.*
23. *The White Paper, p. 30.*
24. *The White Paper, p. 30.*
25. *Ibid.*
26. *The White Paper, p. 29.*
27. *The White Paper, p. 52.*
28. *Ibid.*
29. *Ibid.*

Proposed Framework for Online Harm Protection in Nigeria

From the above, the White Paper considers it important that an OHP framework is established in Nigeria to:

1. Mitigate harmful content[30]
2. Protect vulnerable populations[31]
3. Ensure a safe online environment
4. Promote freedom of expression[32]
5. Promote transparency and accountability[33]
6. Call for regulation by big tech giants.[34]

To address online harms in Nigeria, the framework proposes a multifaceted approach encompassing the following:

Balanced Approach

The framework seeks to protect citizens without infringing on free speech, association, and privacy. The framework should also align with international best practices and respect the technical constraints of digital communication while promoting a safe and respectful online environment. For example, E2EE private messaging is excluded from OHP requirements because they are considered similar to private conversations in the physical world and should remain confidential without any surveillance. This approach applies to one-on-one conversations and small groups of up to five (5) people. However, a caveat is expounded when the conversation involves larger groups or takes place in public spaces where the expectation of privacy is reduced/diminished. This is because despite the sender's initial intention, the control over who views or shares the message is reduced, and it may no longer be considered private.

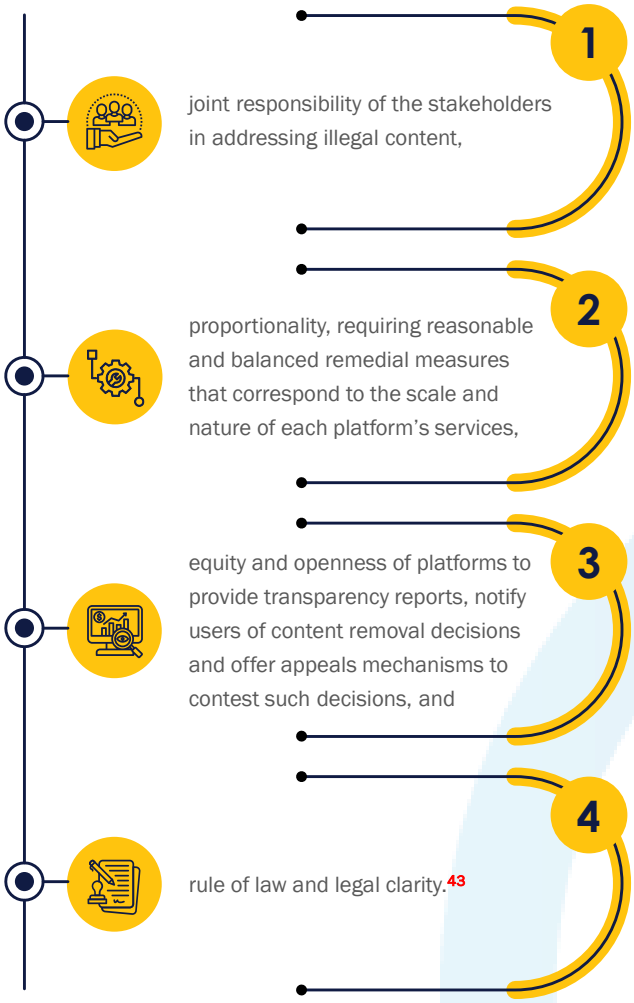
Establishing a Regulatory Framework (the OHP Bill)

The White Paper proposes the enactment of the OHP Bill, which will establish a comprehensive regulatory framework to mitigate online harms while safeguarding the rights of Nigerian internet users. It is proposed that the Bill outlines clear responsibilities and obligations for stakeholders and recognise voluntary and self-regulatory measures as part of a coordinated approach to protect individuals from online harm. A core proposition of the Bill will be the implementation of a duty-of-care model, which places an obligation on platforms to proactively address illegal content and materials that are harmful, particularly to children. This approach will require platforms to adopt preventive measures to mitigate risks while balancing the protection of users' rights to freedom of expression and privacy.

The scope of the Bill will extend to all online platforms accessible within Nigeria, including global platforms and online service providers.[38] The Bill will specifically target providers of user-to-user services, such as social media platforms, dating applications, digital media, and online marketplaces.[39] Platforms enabling user-generated content will be subject to clear thresholds and obligations. Larger platforms with significant user reach or influence will bear additional responsibilities, including CM, transparent reporting, and justification of actions taken.[40] These platforms must also address harmful materials related to children, civic and democratic participation, and journalistic content.[41] This regulatory focus ensures that platforms of varying scales adhere to their responsibilities in safeguarding users from harm.[42]

30. *The White Paper, pp 55-56.*
31. *Ibid.*
32. *The White Paper, pp. 55-56.*
33. *Ibid.*
34. *Ibid.*
35. *The White Paper, p. 61.*
36. *The White Paper, p. 64.*
37. *Ibid.*
38. *The White Paper, p. 65.*
39. *The White Paper, p. 64.*
40. *Ibid.*
41. *Ibid.*
42. *Ibid.*

The regulatory framework will be anchored on four (4) foundational principles:



A key feature of the Bill will be the imposition of strict responsibilities on platforms to combat specific types of harmful content.[44] For instance, platforms will be required to fact-check and promptly remove content such as image-based sexual abuse, cyberflashing, and deepfake pornography. These actions must be carried out within stringent but fair timeframes to ensure that harmful content is addressed swiftly and responsibly.[45]

The Bill will also underscore the importance of a proactive approach in mitigating online harms through regulatory intervention. By addressing the challenges posed by digital misconduct and establishing clear accountability mechanisms, the Bill represents a significant step toward creating a secure, inclusive, and responsible online environment in Nigeria.

Centre for Online Harms Research and Coordination

The White Paper proposes the establishment of the Centre for Online Harms Research and Coordination (the **Centre**).[46] This institution will oversee, enforce, and coordinate the obligations outlined in the OHP Bill. Its primary role is to ensure adherence to the law while promoting transparency, accountability, and the protection of users' rights in Nigeria's digital ecosystem.[47]

The Centre's primary function will be to monitor compliance with the regulatory framework. It will ensure that platforms and stakeholders fulfil their responsibilities under the law, while also coordinating the responses of various public agencies to effectively address online harms.[48] In addition to enforcement, the Centre will lead research efforts, providing insights into the evolving impact of technology on user-generated content both in Nigeria and the sub-region.[49] By conducting and publishing research, the Centre will provide data-driven guidance for future regulations and support best practices that foster a secure and healthy internet space.

As an advisory body, the Centre will offer guidance, advice, and training to the government and private sector on promoting responsible internet use and healthy digital practices.[50] Its role will also include mediating between the need to combat harmful content and the imperative to preserve essential freedoms, such as freedom of expression and privacy.[51] In this way, the Centre will ensure that regulatory actions strike a fair balance between safety and rights in the digital realm.

The governance of the Centre will involve representatives from key government agencies, including the Nigerian Police, the Nigerian Human Rights Commission, the Office of the National Security Adviser, the NITDA, the Nigerian Communications Commission, the Federal Competition and Consumer Protection Commission, and the National Broadcasting Commission. Civil society, academia, and social research organisations will also have representation, ensuring a multi-stakeholder approach to operational oversight and decision-making.[52] This collaborative structure will ensure that diverse perspectives and expertise contribute to the Centre's effectiveness.

43. *The White Paper, p. 64.*
44. *Ibid.*
45. *Ibid.*
46. *The White Paper, p. 66.*
47. *Ibid.*
48. *Ibid.*
49. *Ibid.*
50. *Ibid.*
51. *The White Paper, p. 67.*
52. *The White Paper, p. 66.*

The White Paper proposes that the Centre could be integrated into an existing government agency with an aligned mandate. This approach would leverage established resources and institutional frameworks, accelerating the Centre's deployment and fostering collaboration across the broader ecosystem.[53] Funding for the Centre could be sourced through donations, partnerships, or gifts, ensuring its independence and sustainability while avoiding bureaucratic hurdles.[54]

The Centre will play a pivotal role in coordinating the national response to online harms. It will act as a mediator between combating harmful content and protecting fundamental freedoms, while also providing essential insights and training to stakeholders.[55] By fostering collaboration, promoting transparency, and driving research, the Centre will serve as a cornerstone of Nigeria's efforts to create a safe, inclusive, and equitable digital environment.

Child Online Protection Strategy

The OHP Bill will include a comprehensive Child Online Protection Strategy (the **Strategy**) to safeguard minors in the digital space.[56] The Bill will include an obligation for online platforms to implement robust age verification mechanisms to prevent underage access to inappropriate content and services.[57] By incorporating state-of-the-art technology and best practices, platforms will be encouraged to use effective systems to support age assurance and ensure that age-appropriate materials are accessible only to verified users.[58]

The Bill will also mandate that platforms implement age assurance mechanisms for users under 18 years, with additional restrictions on access to platforms and services for individuals below the minimum age of 13.[59] To address the unique needs of users aged 13-18, it is expected that the Bill will provide that major platforms will be required to develop and incorporate robust parental supervision features such as[60] content filters, time limits, and enhanced privacy settings.[61] The Bill will also emphasise public awareness campaigns to educate parents on using these tools and fostering open communication with their children about online safety. Continuous monitoring and updates of these features will ensure alignment with the evolving digital habits and risks faced by adolescents.[62]

Transparency is a key pillar of the Strategy, with larger platforms required to publish regular risk assessments. These assessments will outline the risks posed to children on their platforms, promoting accountability and informed decision-making by regulators and users.[63]

The Bill will further obligate platforms to actively prevent and remove illegal and harmful content, such as materials depicting child sexual abuse or exploitation.[64] It will require platforms to establish prompt takedown procedures for such content. Instances requiring removal may include disinformation or misinformation that could incite violence or physical harm, as well as harmful content that spreads on digital platforms. Platforms will be encouraged to follow clear policies for content removal and allow for judicial review to ensure fairness and due process.[65] Specific harmful content types that will be addressed in the Bill include false information, hate speech, cyberbullying, image-based abuse, manipulated media and misleading advertisements.[66]

The Bill will also propose the creation of new criminal offences, such as encouraging self-harm, trolling, targeting individuals with epilepsy using harmful flashing content, sharing unsolicited intimate images (**cyberflashing**), and distributing deepfake pornography.[67]

In addition, the Bill will include provisions to grant bereaved parents the legal right to access their deceased child's data on online platforms, ensuring procedural safeguards to respect data protection and individual rights.[68]

53. *Ibid.*
54. *Ibid.*
55. *The White Paper, p. 67.*
56. *The White Paper, p. 68.*
57. *Ibid.*
58. *Ibid.*
59. *Ibid.*
60. *Ibid.*
61. *Ibid.*
62. *Ibid.*
63. *Ibid.*
64. *The White Paper, p. 69.*
65. *Ibid.*
66. *Ibid.*
67. *Ibid.*
68. *Ibid.*

To enhance reporting mechanisms, platforms will be required to provide accessible, user-friendly systems for parents and children to report policy violations.[69]

Finally, the Bill will empower regulatory bodies to impose punishments and sanctions on platforms that fail to comply with its provisions.[70] These measures will align with international human rights standards and global best practices to ensure accountability and compliance.[71] By implementing these measures, the OHB Bill aims to create a safer and more responsible digital environment for children while fostering trust and transparency in the online ecosystem.

COMMENTARY ON THE WHITE PAPER

The White Paper provides a participatory and inclusive approach to proposing the OHP regulatory framework. It ensures that diverse voices, including vulnerable groups, civil society, regulators, and technology companies, are integral to combating OHP. This participatory methodology is a commendable starting point that strengthens the framework's legitimacy and makes it more likely to address the nuanced realities of Nigeria's digital landscape.

The White Paper also draws on Nigerian-specific data and field studies and, at the same time, comparative best practices by leveraging existing international frameworks. This blend of local relevance and global insight enhances the practicality and adaptability of the proposed framework.

In addition, the White Paper provides a holistic and forward-thinking design that focuses on proactive measures beyond traditional CM practices. Another merit of the White Paper is its commitment to balancing the protection of citizens with the preservation of fundamental rights and combining government oversight and platform responsibility for improved governance and accountability.

Despite these commendable aspects, there are still additional areas that the OHP Bill should consider which are not contemplated in the White Paper. These areas are outlined below.

Definition of "Harmful Content" and "Duty of Care"

The White Paper emphasises the importance of clear definition of key terms, obligations and responsibilities in the OHP Bill to provide legal clarity and guide enforcement.[72] In proposing definitions and explanatory notes for key terms, the definitions provided for "harmful content" and "duty of care" are broad and ambiguous. It defines harmful content as "any material encountered online that can cause distress to an individual," with the White Paper adding that it can vary widely and is often interpreted differently based on the subject's cultural, religious and legal context.[73] This subjective definition lacks a clear boundary, leading to potential misinterpretation by regulators and platforms.

Harmful content encompasses a wide range of material, from misinformation and offensive speech to content that is unpopular but not harmful. In defining harmful content, the White Paper provides examples (content that promotes violence, hate speech, discrimination, harassment, bullying, disinformation, misinformation graphic or explicit material and content that glorifies harmful behaviours); however, the language used implies that the examples are non-exhaustive, which may lead to vagueness and ambiguity in interpretation. Also, some examples, such as "misinformation" or "content that glorifies harmful behaviours," are broad and could include a wide range of material.

This broad definition risks overregulation, potentially stifling free speech and creating an atmosphere of self-censorship among users. The OHP Bill needs to clarify whether the intention is to make all subjective "harmful content" punishable or to carve out an objective standard for determining punishable harmful content.

To address these issues, the OHP Bill should propose an objective framework for harmful content, with categories, each accompanied by clear thresholds for enforcement. Providing specificity will help ensure consistent interpretation and enforcement while protecting freedom of expression.

69. *Ibid.*
70. *Ibid.*
71. *Ibid.*
72. *The White Paper, p. 70.*
73. *The White Paper, p. 15.*

Similarly, while the concept of duty of care emphasises proactive measures by platforms, its broad framing leaves uncertainty about the extent of the platforms' obligations. Questions remain about how platforms should balance harm prevention with users' rights, such as privacy and freedom of expression. This could lead to inconsistent enforcement, with smaller platforms or startups being disproportionately affected compared to larger, well-resourced entities.

To clarify, the White Paper could recommend a tiered enforcement approach based on content severity. For example:

Low-Level Harms: These should require user warnings or reduced visibility for flagged content, such as misinformation that does not pose an immediate threat.

High-Level Harms: These mandate immediate removal and notification to relevant authorities, particularly for content like child exploitation material or incitement to violence.

Clarity in defining these key terms is essential to prevent regulators or platforms from exploiting vague definitions to suppress dissent, target political opposition, or remove legitimate content under the guise of harm prevention. Also, inconsistent interpretation by different stakeholders may result in a lack of trust in the regulatory framework.

The Exclusion of E2EE Messaging

In proposing the framework for OHP, the White Paper excludes E2EE private messaging services from the regulatory ambit of OHP for the reasons already highlighted in this article. While this exclusion acknowledges the importance of privacy, the distinction between public and private messages could easily

become blurred. Importantly, privacy and safety need not be diametrically opposed, as there may arise lawful reasons for state intervention in the interests of public safety, similar to the offline world.

Given the potential for private messages to transition into public domains, some messages initially considered private may not be subject to E2EE when shared further, depending on the recipient's understanding or the content's nature. For example, this concern arises prominently in the propagation of fake news, misinformation, and communication bordering on political speech. To address this, the framework should distinguish between the status of a message "at rest" and "in motion" when determining whether E2EE private messaging falls within the regulatory ambit of OHP.

The White Paper's focus on platforms catering to users aged 13-18 years is commendable, particularly its call for collaborative partnerships to develop robust parental supervision features. However, while E2EE provides privacy benefits, it could also impair children's safety and, counterintuitively, weaken their privacy by enabling exploitation or harm.[74] A balanced approach is necessary to safeguard both children's and adults' rights. The proposed framework predominantly emphasises data privacy benefits without adequately addressing safety risks. The inclusion of E2EE private messaging under the OHP framework, along with mitigating measures, should be considered as part of the OHP Bill to achieve this balance. Measures such as metadata analysis, safety-focused encryption models, or lawful access for extreme cases like child exploitation or imminent threats could help address E2EE risks without unduly compromising privacy.

74. *End-To-End Encryption – NSPCC e2ee-pac-report-end-to-end-encryption.pdf accessed 23 January 2025.*

The Practicability of the Duty-of-Care and Intermediary Liability Approach

The framework's duty-of-care and intermediary liability approach lacks clear metrics to assess intermediary compliance and does not specify the extent to which intermediaries are entitled to safe harbour protection from liability for third-party content. While it appears intermediaries are expected to conduct due diligence or implement content moderation measures, the standard for what constitutes "sufficient" action remains undefined. In light of this, we propose that the framework incorporate clear yardsticks or metrics to track compliance and clarify the scope of safe harbour protection available to intermediaries.

Balancing Inter-Regulatory Oversight in Adopting an OHP Framework

While the proposed framework recognises the importance of a co-regulatory approach in combating online crimes, it does not identify the appropriate agency with overarching power on OHP matters. Given that the adoption of an OHP framework may overlap with different agencies and regulatory bodies, it is important that there is a central regulatory oversight. For this reason, the framework proposes that a Centre oversees and enforces the obligations created in the Bill and coordinates the response of public agencies to protect online safety.

While the White Paper proposes that the Centre will operate mainly as a research and coordination institute, this creates a gap in enforcement authority, as the White Paper is also silent on what happens when there is a regulatory overlap on matters bordering on OHP.

Against this backdrop, we recommend that the NITDA should be empowered as the lead agency with the clear authority to regulate and enforce the protection of online harms in Nigeria. In cases of regulatory overlap, NITDA should serve as the point of recourse. International models—such as Australia's eSafety Commissioner—could serve as useful benchmarks for combining research, regulatory, and enforcement functions within a single institution.

CONCLUSION

As digital technologies continue to evolve, strengthening the safety and privacy of Nigeria's digital space will be vital in ensuring OHP in Nigeria.

The White Paper is a good step towards tackling and mitigating harmful content, ensuring a safe environment, promoting transparency and accountability, protecting vulnerable populations, and promoting freedom of expression. It reinforces the government's commitment to ensuring the safety and rights of the digital space.

While the strategies set out in the Whitepaper to achieve a regulatory framework for OHP are laudable, there remain areas of improvement that should be featured in the OHP Bill when eventually issued, some of which have been highlighted in this article.

FOR MORE INFORMATION, PLEASE CONTACT :

Damilola Salawu,
Partner
dsalawu@olaniwunajayi.net

Hopewell Nwachukwu,
Senior Associate
hnwachukwu@olaniwunajayi.net

Opeyemi Araromi,
Associate
oararomi@olaniwunajayi.net

Elizabeth Layeni,
Associate
elayeni@olaniwunajayi.net

Olufolajimi Otitoola,
Associate
ootitoola@olaniwunajayi.net

Ifeoluwa Adeniran,
Associate
iadeniran@olaniwunajayi.net