Internet Impact Brief

Nigeria's Protection from Internet Falsehood and Manipulation Bill 2019

Verengai Mabika, Internet Society
Emmanuel C. Ogu, The #DearGovernments Organization and Internet Society Nigeria Chapter

Version 1.0 (February 2022)

Abstract

Nigeria introduced the "**Protection from Internet Falsehood and Manipulations Bill 2019"** also known as the **Social Media Bill** to the Senate for debate in November 2019. The Bill seeks to criminalise the use of social media in peddling false or malicious information. If passed, the bill would give authorities arbitrary powers to shut down parts of the Internet and limit access to social media. In June 2021, the Government of Nigeria suspended, indefinitely, the operations of the social networking service, Twitter for close to six months till January 2022. These concerns have ignited the Government's interest to implement the proposed Bill. It is within this context that this Report uses the Internet Impact Assessment Toolkit (IIAT) to assess how the Social Media Bill in Nigeria may affect the global Internet by impacting what the Internet needs to thrive as an open, globally connected, secure, and trustworthy resource for all.

The reports finds that implementing the regulatory measures described in the proposed Protection from Internet Falsehood and Manipulation Bill 2019 would negatively affect the performance, resilience, trustworthiness and security of the Internet; with significant impact on the Critical Properties of the Internet Way of Networking. It could also reduce future socio-economic opportunities that the Internet could offer for Nigeria by limiting global access to information by Nigerian citizens, and cutting them off from participating in online spaces.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.

To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally-connected, secure and trustworthy resource.

Context and Assumptions

Nigeria is Africa's largest ICT market, with 82% of the continent's telecoms subscribers and 29% of Internet usage. The country is uniquely positioned to reap the benefits of the digital economy. Nigeria accounts for 47% of West Africa's population, and half of the country's 208 million people are under the age of 30. Nigeria has the largest mobile market in Sub-Saharan Africa, supported by strong mobile broadband infrastructure and improved international connectivity. Nigeria is also home to several high-growth digital companies that provide hopeful examples of the country's digital potential, with ICTs contributing 12.5% to the GDP in 2020.

While Nigeria presents huge opportunities in the digital space, the intentions to regulate social media through the Internet Falsehood and Manipulation Bill present some obstacles and challenges in building an open, globally connected, secure and trustworthy Internet for all.

The proposed bill aims to prevent the transmission of false statements of fact, whether by an individual, or a non-individual (corporate) entity, and make it possible for counter-actions to tackle the consequences of such transmissions. It also aims to destabilize the funding and promotion of "online locations" (social media accounts, websites, and other Internet sources) that frequently transmit false information, and establish measures for detection, control, and protection against bad behaviour that could be propagated by such online locations. The bill also seeks to improve the disclosure of information on sponsored content that serve political purposes; with the provision of penalties for the sanctioning of all categories of offenders.

More specifically, the bill has provisions that: prohibit the transmission of false declarations of fact over the Internet, and creates regulations for dealing with instances of such transmission; regulate the actions and responses of Internet intermediaries and mass media service providers that offer and host Internet services, and close online locations that are found to be in contravention (especially repeatedly) of applicable regulations specified within the Bill.

Relevant Regulatory Provisions

This section highlights specific regulatory provisions that could harm the Internet Critical Properties and the enablers and also describes our interpretation of selected provisions.

1. **Access Blocking order - PART 5, Section 27 [3][4][5]** of the proposed Bill specifies that an online location can be flagged (banned) for repeatedly contravening the regulations, for a period that could reach up to two (2) years. The section specifies that the law enforcement department, in this case the Police may direct the Nigeria Communications Commission (the regulator) to

order the Internet access service provider to take reasonable steps to disable access by end-users in Nigeria to the online location. Our interpretation of this provision can be seen in two possible scenarios:

i) in the case that the online location is a service, website or platform, the content to be blocked is identified by a specific IP address, a domain name or a URL, and

ii) in the case of an online location understood to be a user account, the content to be blocked would need to be identified using platform specific identifiers (e.g. a user ID).

Although the provision does not specify a blocking method, depending on the nature of the blocked content, the content-blocking measures by operators in scenario i) would include IP and protocol-based blocking, deep packet inspection (i.e. viewing content of "packets" as they move across the network), and URL and DNS-based blocking depending on online location.

2. PART 4, Sections 17 and 18: According to the specifications of the Targeted Correction Regulation, an Internet intermediary (providers of DNS resolution services and Internet Service Providers) can be mandated to transmit a declaration that a given statement of fact is false or to specify the source/location where that statement of fact can be found. In doing so, Internet intermediaries must transmit the correction notice to all end-users who have access (or who it knows to have access) to the subject material.

   Our interpretation of this provision is that the regulator impose mandates on the access providers to perform DNS blocking and redirection.

3. PART 4, Section 23: An Access Locking Order is a directive issued by the law enforcement department (the Police) to the Nigerian Communications Commission (NCC) to order an Internet intermediary or mass media service provider to "take reasonable steps to disable access by end-users in Nigeria to the online location", which the NCC must issue (Section 23[2]). This Order is issued in the event that an Internet intermediary fails to comply with a Part 4, section 17 and 18. Note that this differs from the *Access Blocking Order* (specified in PART 5, Section 27 [3][4][5]), which is invoked against declared online locations that have been discovered to be transmitting "harmful or illegal content" in Nigeria after a "declaration" has been issued against them, and when such content has been accessed by end-user(s) in Nigeria after the "declaration" was issued.

   Our interpretation of this provision (the Access Locking Order) is that the regulator can direct Internet intermediaries and mass media providers to block (basically, enforce an Access

Blocking Order against an entity that is presumed to be non-Individual) the online locations flagged by the regulator as transmitting illegal content.

How Does the Proposed Bill Affect the Internet's Foundation?

In order to understand how the proposed Social Media Bill affects the Internet model we assess how it might impact the Critical Properties of the Internet, as described by the Internet Society.

Critical Property 4: **Common Global Identifiers** which are unambiguous and universal

The access blocking provision notes that the regulator, after declaring an online location, can instruct ISPs to block an entire domain when the online location is a website. A common way this has been achieved in other jurisdictions is to make configuration changes at its DNS resolver[1]. When a user asks to access a particular website, the DNS resolver of the customer's ISP recognizes the domain as a blocked site, does not allow it to be translated into an IP address, and responds to the user that the domain does not exist or provides a modified IP address that redirects users to a webpage declaring that the domain is blocked.

DNS blocking affects the globally consistent namespace, a fundamental building block of the Internet. Manipulation and interference with the resolution of DNS records breaks the integrity of the DNS system, with long-term effects that reduce the reliability, openness, and usability of the global Internet. Fracturing the name space creates additional costs, overhead, and friction within the network. Such interference is also likely to include "collateral damage" due to the risk of over-blocking as a single domain can host many websites through website extensions.

Furthermore, the **Access Blocking order as described in PART 5, Section 27 [3][4][5]** also points to IP blocking as an enforcement method. Similar to the case of enforcement using the DNS, such blocking methods interfere with the global identifiers of IP addressing, and could result in "collateral damage" by over-blocking many more than the intended sites or services.

[1] The DNS **resolver** (also referred to as a recursive DNS server) receives queries from the user application and traverse the DNS hierarchy tree by querying the authoritative servers for each sub-domain, starting from the "root" of the requested name to translate it (or "resolve") into one or more DNS records. A typical record is an IP address associated with the requested name, such as an IP address of a website.

How Does the Proposed Bill Affect the Realization of the Full Potential of the Internet?

The critical properties are what is needed to have the Internet, but they are not sufficient if we want the Internet to reach its full potential. In order to assess how we get to an Internet that is Open, Globally Connected, Secure and Trustworthy we will look at these through the lens of the "enablers" of these goals.

Easy and Unrestricted Access

Description: It is easy to become part of the Internet, for networks and users alike. That means that for users the Internet is affordable and Internet services are accessible, and that network operators can easily become part of the Internet, without unnecessary regulatory or commercial barriers for both groups.

The social media bill and the blocking of online services would negatively affect the easy and unrestricted access enabler. The recently lifted Nigerian Twitter ban—enacted after the platform deleted a tweet by President Buhari that it deemed to have breached its terms of service - is an illustration of an infringement of this enabler as it restricts Nigerian users' access to a specific service, but in the event that a service located in Nigeria is blocked, it also prevents that service from being part of the Internet at all.

Unrestricted Use and Deployment of Internet Technologies

Description: The Internet's technologies and standards are available for adoption without restriction. This enabler extends to end-points: the technologies used to connect to and use the Internet do not require permission from a third party, OS vendor, or network provider. The Internet's infrastructure is available as a resource to anyone who wishes to use it in a responsible and equitable way. Existing technologies can be mixed in and used to create new products and services that extend the Internet's capabilities.

The bill risks undermining this enabler by imposing a form of gatekeeping for the social-media-related services, resources, and technologies that power many small businesses and enterprises. For example, end-user applications, services, and utilities that rely on resources

(such as Oauth authentication[2], data, APIs, etc.) or proprietary technologies that are provisioned by a blocked or restricted social media platforms (e.g., Twitter) or other similar websites and platforms. Blocking such resources affects this enabler as it risks interfering with the use of technologies and functionality of other applications.

Unrestricted Reachability

Description: Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties.

The proposed social media ban has implications on which resources a user can use and access, and also restrict the resource the user may contribute to the Internet. Essentially, in Nigeria, as in many African countries, major social media platforms such as Facebook and Twitter are becoming infrastructure services in themselves and are providing additional services. The suspension of Twitter for example created a market access gap for millions of small and medium scale enterprises (SMSEs) that use the platform to reach their customers.

Data Confidentiality of Information, Devices, and Applications

Description: Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet).

Government blocking orders may require that Internet traffic is examined to determine its content. For example, by restricting the use of end-to-end encryption, or by requiring the use of a proxy that decrypts, and/or inspects traffic, before allowing it through. This situation effectively erodes the foundations of trust, transparency, and security that inspires user confidence in the functions and operations of the global Internet.

[2] Many services allow login using a social media account through technology called Oauth. Blocking access to the social media that is used for authentication will likely induce friction for the Nigerian businesses that rely on Oauth to provide their services.

Integrity of Information, Applications, and Services

Description: The integrity of data sent over the Internet, and stored in applications, is not compromised. Critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors. Data stored in applications cannot be manipulated or compromised by third parties.

The blocking or disabling of Internet platforms or services, as empowered by the proposed social media bill, puts this enabler at risk. For example, blocking by manipulating the DNS resolution is in conflict with DNSSEC—a protocol that specifies DNS security extensions and ensures the integrity of the DNS system. By interfering with the answer to the published DNS records, and even "falsifying" the response in the event of a re-direct by pointing the user to a different IP address, it conflicts and undermines the DNSSEC system as a whole.

If DNS redirection is used, it generally discourage the adoption of DNSSEC in the country, which in turn has implications for the integrity of the global DNS system.

Reliability, Resilience, and Availability

Description: The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations.

The fact that the bill effectively excludes the participation of other Internet stakeholders in the decision to block or disable particular Internet services or operations means that a large number of Internet users are likely to learn about the unavailability of a given service at the moment when they need to use it. This weakens the trust that users have in the availability of an Internet service or utility, and undermine confidence in the global Internet itself. Furthermore, there are many online services that depend on functionalities provided by social media platforms, for example for login and authentification. In such instances, the blocking of a social media platform can unintentionally interfere with the reliable operation, and availability, of other services.

Accountability

Description: Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.

The proposed bill confers powers to the police to unilaterally determine what is false and what is not, as well as what can and cannot be shared online - explicitly making the Nigeria Police Force (NPF) responsible for enforcing the provisions of the proposed bill, in interpretation, theory, principle, and practice. Legitimate concerns could be raised about the competence of the NPF to efficiently execute such a sensitive mandate, as well as the probability of arbitrary blocking of content without clear explanations, or transparency, of the decisions[3].

The social media bill contains overbroad provisions that unduly restrict access to and use of social media and seems designed to restrain freedom of expression. For example, section 3, which relates to the transmission of false statements of facts, contains provisions against sharing statements "likely to be prejudicial to the security of Nigeria, public safety, tranquillity, public finances and friendly relations of Nigeria with other countries". This could be easily abused to limit online expression of political views or critique of the government.

In addition, the Twitter ban could be an illustration of what would become more frequent when the Bill becomes law. The Twitter ban was arbitrary and disproportionate: there are no signs that the government pursued more targeted and transparent measures to address the purportedly dangerous content on Twitter. Social media companies such as Twitter have a responsibility to ensure that their platforms are not misused to incite offline violence, which is why Twitter removed President Buhari's post. The government did not consider other options such as a removal request from Twitter. This arbitrary action of the government also raises accountability questions pertaining to the powers of the government to unilaterally rule on whether particular content on the Internet is true or false.

[3] Improving transparency as to why an online location is unavailable can be achieved by the content provider using a signalling mechanism to communicate the reason for the content being blocked (so-called code 451, RFC7725). However, if cooperation with the content provider is not expected the block would be enforced by another entity along the access path (e.g. the ISP). In such instances the code 451 can still enhance transparency, but the negative impact from blocking or re-directs described in previous sections persists.

Summary and Conclusions

Implementing the regulatory measures described in the proposed bill would negatively impact foundational parts of the Internet through interference with its common global identifiers. It would also affect the Internet's openness by limiting the unrestricted use and deployment of Internet technologies, and through restrictions on reachability and accessing the Internet.

Furthermore, while the intention of this bill is to improve the trustworthiness of the Internet the effect is likely to be the reverse. For example, the provisions would threaten Internet security by negatively affecting data confidentiality and the integrity of information, and its impact on reliability, resilience, and availability, as well as accountability, are in direct conflict with a trustworthy Internet.

At the same time, there is little evidence that the measures being conceptualized in the proposed bill would be able to effectively and sufficiently address the problem that is of concern to the bill (i.e., "protection from Internet falsehood and manipulations"). The measures that have been proposed by the Bill can be relatively easily circumvented, which could potentially drag regulators in the unending spiral of the "arms race" against the array of available circumvention techniques, and in turn exacerbate the negative impact.

In sum, these provisions are likely to reduce future socio-economic opportunities that the Internet could offer for Nigeria by undermining its security and trustworthiness, and by limiting global access to information by Nigerian citizens, cutting them off from realities of international relevance.

———————————————————

Acknowledgement

The inputs and participation of the Project Team Members at the #DearGovernments Organization (DearGovs) towards producing the Zero Draft of this Report, are hereby acknowledged: Veronica PICCOLO; Sara El HAMDANI; Abigaël FRANCISQUE; Olalekan Moyosore LALUDE; Amarachi OKONKOH; Moriam O. SULAIMON; and James PAEK.