LEGAL ANALYSIS OF THE PROPOSED PROTECTION FROM INTERNET FALSEHOODS, MANIPULATIONS AND OTHER RELATED MATTERS BILL

Policy Briefing Paper 009

FEBRUARY 2020

SPACES FOR CHANGE | S4C

www.spacesforchange.org

#NoSocialMediaBill: Policy Briefing Paper

INTRODUCTION

Advancements in digital technology have widened exposure and access to modern communication tools, enabling and stimulating people's power and potential to express themselves, organize and engage governments on a wide range of issues. Aided by these tools, governmental behaviour is now more than ever, facing greater levels of scrutiny, and backlash, when things go wrong. Sponsored by Senator Mohammed Sani Musa (APC Niger East), the proposed PROTECTION FROM INTERNET FALSEHOODS, MANIPULATIONS AND OTHER RELATED MATTERS BILL, 2019, is the latest addition to the long list of legislative proposals that hold enormous potential to restrict the civic space and push back on the growing citizens' ability to scrutinize government's actions. This policy brief presents an analysis of the proposed statute, highlighting key concerns in the bill, while proffering recommendations to inform parliamentary deliberations.

MAJOR OBSERVATIONS

1. The bill reproduced several sections of the Cybercrimes (Prohibition, Prevention, Etc) Act of 2015, with only minimal modifications here and there. The Cybercrimes Act,
   in its broadest sense, covered the field regarding false statements and expressions published or disseminated through the social media.

2. The bill is replete with vague phrases framed around the protection of national security, public health, public safety, public finances, bilateral relations with other countries or influencing the outcome of elections to any office and so forth. The language equally used in framing offences in the bill is overly broad that any legitimate, honest expression can be easily stretched to come under the ambit of the stipulated offences.

3. Numerous law enforcement mechanisms for curbing cybercrimes exist. Instead of duplicating agencies to assume statutory roles already being performed by existing law enforcement institutions, the provision of adequate human resources and infrastructure needed to both enhance their technical, investigative and intelligence-gathering skills and strengthen coordination among them, would be a more productive path to follow.

#NoSocialMediaBill: Policy Briefing Paper

OBJECTIVES OF THE SOCIAL MEDIA BILL 2019

Part 1 of the bill details the objectives of the bill. Among other things, it seeks to prevent falsehoods and manipulations in internet correspondences and transmission in Nigeria. The bill's stated objectives are listed below:

- To prevent the transmission of false statements/declaration of facts in Nigeria and enable measures to be taken to counter the effects of such transmission.
- To suppress the financing, promotion and other support of online locations that repeatedly transmit false statements/ declaration of facts.
- To enable measures to be taken to detect, control and safeguard against uncoordinated inauthentic behaviour and other misuses of online accounts and bots.
- To enable measures to be taken to enhance the disclosure of information concerning paid content directed towards a political end.
- To sanction offenders.

HIGHLIGHTS OF THE SOCIAL MEDIA BILL

The bill creates a number of offences and stipulates penalties for violators. They include:

1. **Prohibition of Transmission of False Statements of Facts:** A person may not transmit statements knowing or having reasons to believe they are false, and the transmission of the statements may likely affect the security of any part of Nigeria, be prejudicial to public health, public safety or public finances, or affect Nigeria's relationship with other countries, or influence the outcome of an election to any office in a general election, or incite enmity or hatred towards a person or group of persons, or ill will between different groups of persons. See Sections 3 subsection 1, 2, 3, 4.

2. **Making or Alteration of Bots:** The bill prohibits the making or altering of bots with the intention of transmitting false statements. Anyone guilty of the above offence is liable to a fine of N200,000 or three years imprisonment or both (for individual) **See Section 4 (1).**

3. **Prohibition of Parody Accounts**: Where an inauthentic online account or a bot is used to transmit or accelerate false statements, offenders will be guilty of an offence and punished accordingly. **(See Part 1, Section 3 (3).**

4. **Providing Services for the Transmission of False Statements:** Soliciting, receiving or agreeing to receive any material or other financial benefit or inducement for providing any service used to facilitate the transmission of false statements will constitute an offence under the bill. Violators will be liable to a fine of N150,000 or three years imprisonment or both. The penalty doubles to

N300,000 where such statement affects national security or influences the outcome of an election. **(See Section 5)**.

This section, however, excludes acts incidental to the provision of internet intermediary service, tele-transmission service, computing resource service and the likes. **(See Section 5(4)**.

5. A law enforcement department can issue a **Part 3 Regulations** in the event of a false "declaration" of facts that is being or has been transmitted, or it is in the public interest to issue such declaration. And this declaration will be issued even if the "false statement" has been corrected or pulled down, or ceased to be transmitted. Violators will be required to publish a "correction notice" in a specified form and manner, or to a specified person or persons in any specified online location. **(See Sections 6 & 7 of the Bill).**

6. **Stop Transmission Regulation:** This may be directed at any person, requiring the person to stop transmitting the subject declaration, by taking necessary steps to ensure the DECLARATION is removed from an online location or no longer available on or through the internet to end-users. **(See Section 8).**

   It is important to note that Part 3 Regulations applies to any person within and outside Nigeria and can be served by electronic means. Non-compliance with Part 3 Regulations constitutes an offence. In defence, persons can apply under Clause 19 to vary or cancel the Part 3 Regulations, or apply to the High Court to set aside the Regulations. **(See Sections 10 & 11).**

7. **Access Blocking Order:** This applies where any person fails to comply with Part 3 Regulations**.** Law enforcement departments (the Nigerian Police Force) will have the power to issue an access blocking order by directing the Nigerian Communications Commission (NCC) to order the internet service provider to disable access to users in the online location that false communication emanated from. When this directive is issued, the NCC must give the internet access service provider an access blocking order. **(See Section 12).**

8. **Effects of Non-compliance with Blocking Orders:** An internet service provider that does not comply with an access blocking order is liable on conviction to a fine not exceeding ten million naira for each day during any part of which that order is not fully complied with, up to a total of five million naira. **(See Section 12 (4).**

REPETITIVE ATTEMPTS TO CONTROL DISSENT ON THE SOCIAL MEDIA

In 2016, the *Bill for an Act to Prohibit Frivolous Petitions,* popularly known as the Anti-Social Media Bill, surfaced in the Nigerian legislature, introduced by Senator Bala Ibn Na'Allah. Through sustained advocacy and mass actions coordinated both online and offline, Nigerian activists, active citizens and civil society actors vehemently opposed the bill because of the manifest potential to gag free speech. Yielding to public pressure,

the Nigerian Senate rejected the bill on the 17th of May, 2016, and suspended all further consideration of the proposed law.

Reintroducing the bill after the first failed attempt, the "*Protection from Internet Falsehoods and Manipulations and Other Related Matters Bill 2019"* scaled through the first reading on November 5, 2019. Few weeks later, the bill quickly went through the second reading at the Nigerian Senate on November 20, 2020, reflecting the serious attention and importance accorded to the proposed statute by the Nigerian parliament.

As with the previous statute that failed to secure legislative approval, the primary aim of the new bill is to regulate Nigeria's online space, an aim already addressed by existing legislations. For instance, Nigeria passed the Cybercrimes (Prohibition, Prevention, Etc) Act in 2015, signed into law by former President Goodluck Ebele Jonathan. The Cybercrimes (Prohibition, Prevention, Etc) Act of 2015, in its broadest sense, covered the field regarding communications and expression published or disseminated through the social media.

KEY CONCERNS IN THE SOCIAL MEDIA BILL 2019

1. The Bill Reproduced Several Sections of the Cybercrimes (Prohibition, Prevention, Etc) Act of 2015

Juxtaposing the provisions of the Cybercrimes Act of 2015 with the proposed Social Media Bill 2019, SPACES FOR CHANGE notes that they not only share similar objectives, but their provisions are also markedly repetitive. Not only that, some provisions of the Social Media Bill reproduced certain sections of the Cybercrimes Act verbatim, with only minimal modifications here and there. We highlight some of the repetitions below:

1. Section 22 subsection 2, 3 (a-d) and 4 of the Cybercrimes Act provide that:

> *(2) Any person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person; or*
>
> *(3) fraudulently impersonates another entity or person, living or dead, with intent to –*
>
> *(a) gain advantage for himself or another person;*
>
> *(b) obtain any property or an interest in any property;*
>
> *(c) cause disadvantage to the entity or person being impersonated or another person; or*
>
> *(d) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.*
>
> *(4) any person who makes or causes to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied upon respecting his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or another person commits an offence and shall be liable on conviction to imprisonment*

for a term of not more than 5 years or a fine of not more than N7,000,000.00 or to both such fine and imprisonment.

The above provision of the Cybercrimes Act is far-reaching, covering issues pertaining to the transmission of false statements, use of parody accounts to transmit false communication, soliciting and receiving any service to facilitate the transmission of false statements and the obstruction of justice. It went further to impose stiffer penalties for any breach of these provisions. Sections 1, 3, 4 and 5 of the Social Media Bill merely regurgitates Section 22 of the Cybercrimes Act 0f 2015, with minimal modifications.

Section 26 (1) a-d of the Cybercrimes Act provides that:

> *(1) Any person who with intent –*
>
> *(a) distributes or otherwise makes available, any racist or xenophobic material to the public through a computer system or network;*
>
> *(b) threatens through a computer system or network –*
>
> *(i) persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors; or*
>
> *(ii) a group of persons which is distinguished by any of these characteristics;*
>
> *(c) insults publicly through a computer system or network–*
>
> *i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or*
>
> *(ii) a group of persons which is distinguished by any of these characteristics; or*
>
> *(d) distributes or otherwise makes available, through a computer system or network, to the public, material which denies or approves or justifies acts constituting genocide or crimes against humanity, Commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more thanN10,000,000.00 or both such fine and imprisonment.*

As equally espoused in Part 2 of the Social Media Bill, the above provision of the Cybercrimes Act prohibits statements with the potential to incite racism, ethnicism, enmity or hatred towards a person or group of persons, or cause ill will between different groups of persons. Section 24 of the Cybercrimes Act takes a further step to criminalise the transmission of messages or statements by means of computer systems or network, especially when they are false, or cause annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another.

The cybercrimes law is so expansive that it proscribes other incendiary acts such as bullying, threatening or harassing another person, where such communication places another person in fear of death, violence or bodily harm.

3. Section 40 of the Cybercrimes Act is also similar to the access blocking order provision of the Social Media Bill. Section 40 of the Cybercrimes Act provides:

> *(1) It shall be the duty of every service provider in Nigeria to comply with all the provisions of this Act and disclose information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding under this Act.*
>
> *(2) Without prejudice to the generality of the foregoing, a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards–*
>
> *(a) the identification, apprehension and prosecution of offenders;*
>
> *(b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or*
>
> *(c) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.*

Service providers who violates this provision not only commit an offence, but also, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than N7,000,000.00 or to both such fine and imprisonment.

2. Bill Contains Overly-broad, Vague Provisions that Undermine Human Rights

The bill is replete with vague phrases framed around the protection of national security, public health, public safety, public finances, bilateral relations with other countries or influencing the outcome of elections to any office and so forth. The language equally used in framing offences in the bill is overly broad that any legitimate, honest expression can be easily stretched to come under the ambit of the stipulated offences. For instance, there are no parameters for measuring when a statement has influenced election outcomes or hurt the bilateral relations between Nigeria and another sovereign nation. A standard-setting guide can help internet users to for instance, establish clear links between online expressions and electoral outcomes.

Furthermore, the interpretation section of the bill is silent on the definition of these terms. Where the benchmarks for measuring compliance or violation are missing, legal provisions could be prone to abuse, especially by interpreting or applying them beyond the original intendment of the law in order to justify crackdowns on civil society, including targeted attacks on activists, journalists, bloggers, and civil society organisations. A case in point is the arrest of a blogger, Mr. Abubakar Sidiq Usman, in August 2016, by the Economic and Financial Crimes Commission, EFCC, for writing unflattering stories about the EFCC chief executive.

Though arrested for cyber stalking and later released, he was the third blogger to be arrested since the Cybercrime Act came into force in 2015. In all the three cases, the

2015 Cybercrime Act was invoked to justify the arrest and prosecution of bloggers on account of their online expressions on social media. These incidents portray an official disposition to use legal rules to achieve pre-determined outcomes, perpetuate institutional self-interests, and clog the wheels of civic freedoms.

3. Numerous Law Enforcement Mechanisms for Curbing Cybercrimes Exist

A number of law enforcement agencies are statutorily mandated to tackle cybercrime. They include the Cybercrime Advisory Council, the National Computer Forensic Laboratory, the National Computer Emergency Response Team (CERT) Coordination Center and the National Human Rights Commission (NHRC). More specifically, Nigeria constituted the 31-person Cybercrime Advisory Council to tackle rising criminal activities and to protect the nation's cyberspace. The Council has the responsibility to formulate ways of implementing the Cybercrime Act of 2015.

On the other hand, the NHRC's mandate includes dealing with all matters relating to the promotion and protection of human rights as guaranteed by the Constitution of the Federal Republic of Nigeria, and other international and regional instruments on human rights to which Nigeria is a party. Offences relating to ethnic hatred or statements causing ill-will between persons and groups infringe Nigeria's constitutional protections for the rights to life, privacy and non-discrimination, bringing any violations against such rights within the purview of NHRC. Not only that, Nigeria has robust legal regimes prohibiting defamation, seditious publication, libel, slanderous comments, all of which involve the transmission of false statements about other persons or institutions. Instead of duplicating agencies to assume statutory roles already being performed by existing law enforcement institutions, the provision of adequate human resources and infrastructure needed to both enhance their technical, investigative and intelligence-gathering skills and strengthen coordination among them, would be a more productive path to follow.

CONCLUSION

SPACES FOR CHANGE lauds the efforts of the bill's sponsor, Senator Muhammad Sani Musa, to contribute to nation-building by proffering solutions for ending criminal activities perpetrated on internet platforms or through the use of electronic and computing systems. However, the multiplicity of laws hampers the development of democratic processes by encouraging the waste of scarce public funds, weakening existing institutions and creating excessively complicated administrative procedures for law enforcement.

In light of the above, SPACES FOR CHANGE recommends as follows:

- **Strengthen the capacities of existing law enforcement agencies statutorily mandated to tackle cybercrime, particularly the Cybercrime Advisory Council, the National Computer Forensic Laboratory, the National Computer Emergency Response Team (CERT) Coordination Center and the**

National Human Rights' Commission (NHRC) by providing them with adequate human resources and infrastructure needed to both enhance their technical, investigative and intelligence-gathering skills and strengthen coordination among them.

- **Accelerate the implementation of existing cybercrime laws and policies, especially the Cybercrimes (Prohibition, Prevention, etc) Act 2015, and the National Cyber Security Policy and Strategy, adopted on the 5th of February, 2015**
- **Ensure the conformity of Nigeria's cybercrime and cybersecurity laws and policies with regional and international human rights standards.**

- **Efficiently utilise the National Orientation Agency and the Ministries of Information across the various levels of government to deliver mass sensitization campaigns to counter fake news, hate speech and ethnic hatred.**

- **Innovating and strengthening community/ grassroots-based policing networks across the federation.**

For further information, please contact:

- Victoria Ibezim-Ohaeri
- Olusola Mercy Olutayo

Office: 35B Ajakaiye Street, Onipetesi Estate, Mangoro, Ikeja, Lagos

Email: spacesforchange.s4c@gmail.com | info@spacesforchange.org

Website: www.spacesforchange.org

Telephone: +2347036202074 | +2349094539638

Twitter: @SPACES4CHANGE