MEMORANDUM

Centre for Democracy and Development

March 04, 2020

TO: The National Assembly

FROM: The Centre for Democracy and Development (CDD)

SUBJECT Protection from Internet Falsehood and Manipulation Bill 2019 (SB 132)

The Protection from Internet Falsehood and Manipulation Bill, 2019 (SB 132), passed the second reading of the Senate in November 2019. Leading the debate on the Bill at the plenary session, Sen. Mohammad Sani Musa (APC: Niger) explained that the Bill aims to mitigate the threat of false information spread on the internet by monitoring online spaces. Considering the increasingly important role internet activity plays in determining citizen wellbeing, interventions to control such activity must be wholly justified. After research and review of the Bill, CDD has concluded that the Bill should not pass. IN this memorandum CDD outlines three main arguments against the Bill's passage and suggests three alternative courses of action.

Cases against the Protection from Internet Falsehood and Manipulation Bill

1. A Business Case

Nigeria needs to diversify its economy. By stifling internet access for online businesses, access blocking orders can inadvertently work against this diversification.

Internet access promotes economic growth in Nigeria. Online platforms, including social media platforms, make it possible for small and medium sized enterprises (SMEs) to locate and transact with customers. An "access blocking order" as found in Clause 12, subclause 3 empowers the Law Enforcement Department to "direct the NCC [Nigerian Communications Commission] ... to order the internet access service provider to take reasonable steps to disable access by end-users in Nigeria."

The Bill is ambiguous about how targeted the disabling of access by end users will be; however, access blocking orders can stifle economic activity at any level of granularity. Access blocking orders will interfere with business operations of these SMEs if the orders block social media platforms. CDD surveyed Nigerians' social media habits in late 2019 and early 2020; platforms such as Instagram and Facebook doubled as online businesses for many respondents.

Furthermore, blanket access blocking orders will affect businesses for whom internet access is an important part of their business model even if they do not transact via social media. In 2017, Cameroonian authorities repeatedly shut off access to the internet in certain regions of the country. Innovation hubs, education and healthcare services and money transfers, which rely on internet access, were negatively affected to the tune of more than $38 million.1 We question whether the potential economic tradeoffs associated with access blocking orders are justifiable?

2. A Human Rights/Democratic Case

The Bill does not provide for a standard of effective investigation in the determination of contraventions of its provisions. A low burden of proof coupled with the scope for subjective judgements is a recipe for abuse that could ultimately contravene freedom of speech. This is worsened by an under-resourced and digital-apathetic police force, who are unlikely to use a publicly available methodology for selecting cases. Furthermore, targeted correction regulations go against data privacy norms in certain areas.

The Bill provides for a low burden of proof in the determination of contraventions of its provisions. For example, the Bill provides for subjective judgement as to whether the transmission of false statements of fact is likely to, amongst others, incite feelings of enmity, hatred towards a person or ill-will between groups of persons. Providing for subjective judgements without a standard of effective investigation opens up the Bill to abuse. Such abuse will ultimately contravene freedom of expression as protected under Section 39 of the 1999 Constitution and Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which Nigeria is a signatory.

There is a more explicit consideration for burden of proof in the case of varying or canceling a regulation issued; clause 15 subclause (2) provides that "the Law Enforcement Department may vary or cancel the Part 3 Regulation under sub Clause (1)...on the Law Enforcement Department's own initiative provided there is overwhelming sufficing evidence necessitating this variation or cancellation" (emphasis added). The burden of having "overwhelming sufficing evidence" should apply at both the introduction and the withdrawal of a regulation, and the process for establishing this evidence should be explicit and rigorous.

The designation of the Nigerian Police Force (NPF) as implementer of the Bill is operationally dubious. Implicit in the Bill is that NPF is expected to surveil the entire Internet to identify false statements. An NPF which the Inspector General of Police and Police Service Commission have both stated is grossly underfunded and understaffed is unlikely to discharge this duty adequately.[2] Additionally, if one takes the funding proposal it recently submitted to the House of Representatives as an indicator of its priorities, the lack of a request for funds to enhance digital capacities is telling.[3] An under-resourced and digital-apathetic NPF suggests the methodology for selecting false statements of fact will be open to political influence, contravening Section 17 of the 1999 Constitution which enshrines equality before the law.

Finally, the exercise of "targeted correction regulation" may go against best practice data privacy principles. Directing internet intermediaries to send correction notices to all end users who accessed a false statement or subject material via their platform can amount to an unethical tracking of user activity.

---

[1]https://www.aljazeera.com/news/2018/01/cameroon-internet-shutdowns-cost-anglophones-millions-180123202824701.html
[2]https://punchng.com/police-need-n944-9bn-to-protect-nigerians-says-ig/
[3]Ibid.

3. A Security Case

Nigeria currently has an insecurity problem. Access blocking orders could deter online intelligence gathering through both blocking internet access and possibly stimulating the development of an online information black market.

One of the aims of the Bill, as stated in Clause 1(e) is to "enable measures to be taken to detect, control and safeguard against coordinated inauthentic behaviour and other misuses of online accounts and bots". However, access blocking orders could work against digital surveillance operations for security purposes. The mechanism is clear: this type of censorship removes access to information for end users, stopping them from interacting online and providing digital evidence of coordination of both disinformation and higher security alert operations. The nature of security operations does not allow for certainty, but one can reasonably assume that online intelligence gathering has come to form an integral part Nigerian security agencies' defence strategies.

Furthermore, the use of the access blocking orders could inadvertently stimulate the development of an online information black market. The technologies internet service providers use to restrict internet access can be circumvented through the use of VPNs, TOR and other online privacy tools. In 2018, Cameroonian authorities ordered an internet shutdown of Anglophone regions, which resulted in many citizens taking to these privacy tools to circumvent the shutdown.[4] Use of privacy tools would further conceal digital interactions and hinder security operations.

Alternatives to the Protection from Internet Falsehood and Manipulation Bill

1. Demand side (end-user) interventions[5]

In focusing on those who produce and distribute disinformation, the Bill represents a supply-side intervention. However, given the decentralized nature of disinformation's production, a supply-side intervention amounts to cutting the head off a hydra. A robust response would consider interventions to bolster the end-user's ability to critically engage with and judge the veracity of information. The demand for disinformation is driven by the psychology of news consumption and opinion formation. The disconfirmation bias suggests that people are unlikely to accept information that conflicts with their pre-existing beliefs. Thus, correction notices[6] are likely to be viewed as government-controlled media and may even reinforce beliefs that false stories are true. Rather than getting involved directly, the government should fund critical thinking and digital literacy training for both child and adult education. Such critical thinking training should explicitly address the biases that contribute to the demand for disinformation. Beyond national and state education ministries, the National Orientation Agency could seek to introduce awareness of and techniques to mitigate these biases into the national consciousness.

[4]https://www.aljazeera.com/news/2018/01/cameroon-internet-shutdowns-cost-anglophones-millions-180123202824701.html
[5]This section draws heavily from https://www.ned.org/demand-for-de-ceit-how-way-we-think-drives-disinformation-samuel-woolley-katie-joseff/
[6]A provision of the Bill (Clause 7) that involves a person found to declare false statements declaring that the false statements are indeed false and including the actual fact in the situation and/or where to find it.

Ibid.

2. Fake-news-proofing platform algorithms[7]

Disinformation is inadvertently fueled by the algorithms that sort search results and the feeds or docking pages of many social media platforms. While the specific features that form the weights of the algorithms are typically unknown, it is evident that more popular posts or results are more likely to be prominently displayed. Unfortunately, fake news posts are often designed to "go viral" with the aim of appearing on as many people's feeds as possible. But social media platforms and search engines may not have incentives to introduce adjustments to these algorithms on their own; popularity does drive engagement, and engagement is the core of their business models.

Here the government can step in to mandate technical provisions for algorithms such that they mitigate "gaming", that is, including certain features in posts to stoke virality regardless of veracity. There are also machine learning algorithms that, based on previous instances of news verified as false, predict the falsehood of a given statement with reasonable accuracy.[8] This arena need not, indeed should not, be the exclusive preserve of academics and technologists. Nigeria needs to invest in its technical capacity to understand and contribute to 21st century technologies, because those who spread disinformation are already doing so.

3. Accreditation for content creators

In one of CDD's key informant interviews on the issue of fake news, a senior member of the Nigeria Union of Journalists (NUJ) suggested accreditation of online content creators under their auspices. The official asserted that many of their extant processes for dealing with journalists could benefit online content creators without great modification, including training in norms of ethical journalism and peer-driven sanctions for breaking those norms. This arrangement would also enable the government to deal with the NUJ as the representative for

[7]This section draws from https://law.yale.edu/fighting-fake-news-workshop-report
[8]http://news.mit.edu/2019/better-fact-checking-fake-news-1017

Ibid.

SIGNED:

IDAYAT HASSAN
DIRECTOR CDD

Centre for Democracy & Development
Centre pour la démocratie et le développement

The Centre for Democracy and Development (CDD) was established in the United Kingdom in 1997 as an independent, not-for-profit, research training, advocacy and capacity building organisation.

Address
16 A7 Street, Mount Pleasant Estate, (CITEC)
Mbora District- Jabi Airport Road,Abuja

Phone No
+23492902304

Email
cdd.abv@cddwestafrica.org

Website
www.cddwestafrica.org