

**Submission in Advance of the Review of Nigeria, Human Rights Committee  
126th Session, 1-26 July 2019.**

**Background**

This submission is made by Paradigm Initiative (PI), a social enterprise working on digital inclusion and digital rights advocacy in Africa, with offices in Cameroon, Nigeria, Tanzania, Togo and Zambia. Paradigm Initiative works with local and international partners, and through the NetRights African Coalition which it coordinates, PI monitors and intervenes on issues around human rights online in Africa. Paradigm Initiative submitted a similar report on “Trends in Freedom of Expression in the Telecommunications and the Internet Sector in Nigeria”<sup>1</sup> to the United Nations Human Rights Council in 2016. As part of our research and advocacy work, we have been monitoring developments within the digital rights space and are happy to make this submission to the UN Human Rights Committee ahead of its 126th session. The information provided in this submission derives from our 2018 annual report; Digital Rights in Africa Report<sup>2</sup>, Freedom on the Net Report<sup>3</sup> and State of Privacy in Nigeria<sup>4</sup>, a report we jointly developed with Privacy International in 2018.

**Overview**

The population of **Nigeria** is **200,443,573**<sup>5</sup> 2019, based on the latest United Nations estimates. Internet penetration number is set at 111,632,516<sup>6</sup> representing over 50% of the country’s population. The legal landscape around human rights online continues to be defined by current security challenges and trappings of long years of military rule.

**Communication surveillance and right to privacy (art. 17) 19**

Legal and regulatory frameworks governing communications surveillance and report on its compatibility with human rights standards.

In a 2018 report co-written with Privacy International on the State of Privacy in Nigeria we identified two pieces of legislation authorising communications surveillance in Nigeria: the Terrorism (Prevention) Act 2011 and the Cybercrimes (Prohibition, Prevention, Etc) Act 2015.

---

<sup>1</sup> Paradigm Initiative, Nigeria: Trends in Freedom of Expression in the Telecommunications and the Internet Sector. Available at

<https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/ParadigmInitiativeNigeria.pdf>

<sup>2</sup> Paradigm Initiative, Nigeria: Digital Rights in Africa Report, 13 November 2018. Available at

<http://paradigmhq.org/download/digital-rights-in-africa-report-2018/>

<sup>3</sup> Freedom on the Net 2018 Report on Nigeria. Available at

<https://freedomhouse.org/report/freedom-net/2018/nigeria>

<sup>4</sup> Paradigm Initiative and Privacy International: Stakeholder Report Universal Periodic Review 31st Session - Nigeria, The Right to Privacy in Nigeria, March 2018. Available at

[https://privacyinternational.org/sites/default/files/2018-05/UPR\\_The%20Right%20to%20Privacy\\_Nigeria.pdf](https://privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf)

<sup>5</sup> Worldometers: Nigeria Population (Live). Available at

<https://www.worldometers.info/world-population/nigeria-population/>

<sup>6</sup> Internet World Stats Available at <https://www.worldometers.info/world-population/nigeria-population/>

Despite incorporating some safeguards, both Acts contain insufficient protections for the right to privacy, as they do not comply with the internationally recognised human rights principles that surveillance policies and practices must observe. These include: legality, necessity, proportionality, judicial authorisation, effective independent oversight, transparency, and user notification, among others. These two legislations remain the regulatory frameworks governing communication surveillance as at the time of making this submission

[Surveillance measures and practices undertaken under the Terrorism \(Prevention\) Act of 2011 and the Cybercrimes Act of 2015 vis-a-vis the principles of legality, necessity, proportionality, judicial authorisation, independent oversight and users' notification.](#)

Under the Terrorism (Prevention) Act 2011, law enforcement agencies— with the approval of the Attorney General and the Coordinator on National Security—may apply to a Judge for an “interception of communication order” for the purpose of preventing a terrorist act or prosecuting offenders under the Act. The Cybercrimes (Prohibition, Prevention, Etc) Act 2015 sets out a separate regime for communications surveillance. Where there are “reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may order a service provider (any entity providing access to the internet) to intercept, collect, record, permit, or assist authorities in collecting or recording content or traffic data associated with specific communications, or authorise a law enforcement officer to collect or record the same.

### ***Absence of Test of Necessity or Proportionality***

Neither the Terrorism (Prevention) Act nor the Cybercrimes (Prohibition, Prevention, Etc) Act prescribes such a test of necessity and proportionality and instead grants the authorising judge broad discretion to order surveillance measures. In the Terrorism (Prevention) Act, vague terms compound this concern and allow for a wide interpretation of the types of actions that could justify issuing an order. The Judge is empowered to issue an order for “intelligence gathering,” though the legislation provides little guidance on what qualifies as intelligence, apart from stating that “[t]he law enforcement and security agencies . . . shall be responsible for the gathering of intelligence and investigation of the offences provided under the Act.

[Massive surveillance of mobile phones in the State party's capital; and an increased monitoring of online activities by government actors, particularly on social media..](#)

Allegations of massive surveillance of mobile phones in the Nation's capital appeared in several news reports in 2018, but have not been independently verified. Pronouncements by senior government officials, including army officials, on government plans to monitor social media activity have also been noted. Suspicions that the government indeed has the capability to implement these objectives have heightened following the inclusion of cryptic items into budgetary allocations in the past 3 years. Items in the budgetary allocations under the office of the National Security Adviser and Department of State Services have included provisions for

“Stravinsky project”, which is widely known to be surveillance related; “social media mining suite” and “surveillance drone”.

#### Data protection legal frameworks and regulations:

As at the time of making this submission, no data protection law emanating from the country’s law-making body has emerged although there are pockets of ongoing efforts in the country. Subsidiary legislation in form of the National Information Technology Development Agency (NITDA) Data Protection Regulation<sup>7</sup> has been issued to apply to all transactions intended for the processing of personal data and to the actual processing of personal data and all natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent. This Regulation was issued on the 25th of January 2019 and while the Regulation remains enforceable, there have been agitations for a standard Data Protection Act by the National Assembly. It was however reported<sup>8</sup> that in May 2019, the National Assembly, passed a data protection legislation<sup>9</sup> which now awaits presidential assent to become law. Nigeria’s President Buhari refused to give assent to the Digital Rights and Freedom Bill earlier passed by the National Assembly. The Bill sought to among other things, guarantee privacy within the Interception and surveillance regime. The President clearly indicated in his letter<sup>10</sup> to the Senate, that he didn’t want the Bill to cover such subject as surveillance and interception of communication.

#### Freedom of expression, assembly and association and human rights defenders (arts. 6, 7, 19, 21 and 22)

#### The mandate of the National Broadcasting Commission and on any legal safeguards to ensure that its activities comply with article 19 of the Covenant.

The National Broadcasting Commission (NBC) is the agency of government in Nigeria which is specially tasked with regulating broadcasting services in Nigeria. It has a Code of Conduct document which addresses its relationship and expectation from Broadcasters in Nigeria. While, this code<sup>11</sup>, forbids the use of lewd, profane, pornographic or other vulgar or obscene expression, it clearly tasks broadcasting organizations to use their freedom of expression as agents of the society and not for special, personal or sectional rights, privileges or needs of their own, or of their proprietors, relatives, friends or supporters. One of the factors the NBC will consider in granting license to an applicant is whether such an organization accepts pluralism of ideas and opinion as a guiding principle. In line with this mandate for promoting the pluralism of ideas and opinions. The NBC requires that Broadcasters provide equal opportunity and air time to all political parties or views, with particular regard to amount of time and belt during electioneering campaign period.

---

<sup>7</sup> NITDA: Nigeria Data Protection Regulation, 2019 Available at <https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf>

<sup>8</sup> Adekunle: Vanguard Newspaper, 17 May 2019 Available at <https://www.vanguardngr.com/2019/05/reps-passes-bill-to-make-june-12-democracy-day/>

<sup>9</sup> National Identity Management Commission, Personal Information and Data Protection Bill. Available at [https://www.nimc.gov.ng/docs/reports/personal\\_info\\_bill.pdf](https://www.nimc.gov.ng/docs/reports/personal_info_bill.pdf)

<sup>10</sup> Solomon Fowowe: Guardian NG, Buhari Declines Assent to Digital Rights and Freedom Bill, Four Others, 20 March 2019. Available at <https://guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/>

<sup>11</sup> Nigeria Broadcasting Commission: Nigeria Broadcasting Code Reviewed in 2002. Available at [http://www.nbc.gov.ng/uploads/nbc\\_documents/1466685527-code%20third%20edition.pdf](http://www.nbc.gov.ng/uploads/nbc_documents/1466685527-code%20third%20edition.pdf)

The Commission, however, forbids the expression of personal opinion by a presenter in a broadcasting programme, rather states that such an anchor shall be a purveyor of opinion, and shall not seek to impose opinion on callers.

[Chapter 7, Sections 50 \(2\) and 60 of the 2004 Criminal Act; Disposition towards possible review of legislation regarding libel, slander and defamation by the State.](#)

It has not been observed from the actions, statements and practices of the State party that it has any intentions to review its legislation regarding libel, slander and defamation. Potential legislation, such as the Digital Rights and Freedom Bill which in effect could promote free expression and allow for more dissenting opinion, have been slowed down from coming into existence.

[Provide detailed information on Section 13 \(9\) of the 2016 Digital Rights and Freedom Bill and its use in practice.](#)

It is important to note that the Digital Rights and Freedom Bill is not a law yet. Although the Bill was passed by the Nigeria's parliament, it is yet to become a Law because the President hasn't assented to it. It is therefore impossible to review the use of the Bill in practice at the moment.

[How accusations of libel are used by State authorities in retaliation for negative reporting against journalists; and \(b\) Section 24 of the 2015 Cybercrime Act is used to arrest bloggers critiquing the government.](#)

As documented in our research reports - Digital Rights in Africa Reports (2016 - 2018) and Status of Internet Freedom in Nigeria Report (2016 and 2018), there has been an increase in the number of journalists and bloggers arrested for negative reporting/criticism by the authorities. Sections 24, 37 and recently section 38 of the Cybercrime Act 2015 has been the chief legal justification for the arrests. These sections speak to "cyberstalking and harassment", terms which cannot be said to describe the work of journalists.

[Government official's declarations in 2017 that the military would monitor social media for hate speech, anti-government and anti-security information and how such a declaration could discourage free expression and encourage self-censorship.](#)

Truly, the pronouncement was made that the military would monitor social media for hate speech, anti-government and anti-security information. Civil society organizations have also noticed that such declarations have been backed up by budgetary allocations in recent years to the office of the National Security Adviser and Department of State Security (DSS) for surveillance and social media monitoring equipment. There is no doubt that in an environment already characterized by intimidation of the media and critical voices, such a declaration will discourage free expression and further entrench self-censorship.

Bloggers, journalists, activists and human rights defenders critical of government officials or activities are arrested, detained, tortured, especially when they cover corruption scandals, human rights violations, separatist and communal violence. With regard to human rights defenders

Our Digital Rights in Africa Reports, Status of Internet Freedom in Africa Reports and Freedom House Reports on Nigeria contain the record of the numerous bloggers, journalists, activists and human rights defenders who have been arrested, detained and tortured usually following criticism of government officials or the well connected in society. This is not an allegation, but verified facts. These activists have been detained usually with the legal instruments of Nigeria's Cybercrime Act or libel laws.

Government's intention to adopt legislation or policy measures aimed at recognizing, promoting and protecting the work of bloggers, journalists, activists and human rights defenders.

Much of the provisions towards recognizing, promoting and protecting the work of bloggers, journalists, activists and human rights defenders are already codified in Nigerian law. However these provisions are generally ignored or alternative legal routes found to prosecute civil society. For instance although freedom of the Press is guaranteed in section 39 of the Nigerian constitution, libel laws and the Cybercrime Act of 2015 is still used as a legal route to justify the arrest of activists. Similarly, despite Nigeria having a Freedom of Information Act, requests by Journalists, activists, watchdog bodies and the human rights community are rarely honoured.

## **Conclusion and Recommendations**

The regulatory environment in Nigeria is hardly promoting or improving human rights online, and state-led conversation around laws have been dominated by security concerns and the desire to limit rights in the guise of addressing security challenges. Efforts at improving on the human rights framework are mostly initiated by civil society. The State has not in any way demonstrated strong interest. The National Human Rights Commission, for example, is poorly funded and sometimes lacking in capacity to fulfil its mandate due to resource gaps. It is clear that the hope of protecting human rights and strengthening the legal framework for the protection of human rights online in Nigeria rests largely on civil society and its capability to fill this gap working with stakeholders to advocate for laws that promote human rights online and push back on the unending desire by the state to limit or reduce rights protection in Nigeria. Therefore we are making the following recommendations;

1. That the Government of Nigeria repeal and reenact the Nigeria's Cybercrimes Act 2015 which is the major legal instrument being used to violate the right to freedom of expression of Nigerians: It is important to repeal Section 24 of the Bill as it directly violates citizens right to freedom of expression.
2. That the Nigerian Government should reconsider its position on the Digital Rights and Freedom Bill; A civil society led effort which seeks to guarantee the application of human rights for Nigeria Citizen in the Digital age.
3. That the Government of Nigeria embrace accountability and transparency in its surveillance and Interception regimes and accord data privacy and confidentiality greater priority.

4. That the Nigerian government work and support the efforts of civil society to promote human rights in Nigeria through dialogue, collaboration and effective feedback mechanism without intimidation to actors in the civic space.
5. That the Nigerian government should desist from any act that suggests the closure of the civic space.
6. That the Nigerian Government should sign the Data Protection Bill recently passed by the National Assembly into Law.
7. That the Nigeria government should preserve the plurality of the media space and ensures the National Broadcasting Corporation in fulfilling its mandate, do not gag the media and allows for the propagation of opinions that may pass as dissent and other such opinions that ensures citizens have access to alternative information aside those emanating from the official, government sources.
8. That the Nigerian Government should further empower the National Human Rights Commission and increase budgetary allocation to the commission in order to reduce the resource gaps identified with the commission in fulfilling its mandate.