

A comparative analysis between the Digital Rights and Freedom Bill and other legislation in Nigeria



A comparative analysis between the Digital Rights and Freedom Bill and other legislation in Nigeria

December 2020



About the Author

Ridwan Oloyede. CIPP/E, CIPM, Research Fellow

He leads the privacy, data protection and tech policy team at Tech Hive Advisory. His expertise also includes cybersecurity governance and compliance, and digital ethics. Ridwan advises clients on aspects of global data protection and privacy laws, including regulation compliance, international transfers of data, roll out of new and disruptive technologies, data governance, data localisation, privacy by design, cloud computing and big data, digital health, and global data risk management. He is a Research Fellow at the African Academic Network on Internet Policy (AANOIP). Lexology recognised him as the Legal Influencer for TMT (Technology, Media, and Telecommunication) in Africa and Middle-East for Q4 2018 and recently rated as Top 50 individuals leading in legal innovations in Africa by Africa.

He co-founded Privacy Alliance, an organisation providing businesses with global privacy solutions. He leads the West-African operation.

Dough ONAH holds a Masters Degree in Forensic Science from the University of Ibadan and works as a researcher in the University of Calabar. He is a fellow of the Nigerian School on Internet Governance, Scholar, European Forum Alpbach . He currently serves on the "Non-State Actors Working Group On the 9th Assembly Nigerian Constitution Review Process" led by the Pan African Centre for Social Development and Accountability. He is also the project coordinator for the UNESCO Awareness-raising Campaign on Migration and COVID-19 in West and Central Africa. Project: "Empowering Young People in Africa through Media and Communications", being implemented in eight (8) countries in West and Central Africa: Cameroon, Côte d'Ivoire, Ghana, Guinea-Conakry, Mali, Niger, Nigeria and Senegal.

The research was notably supported with contributions from

Oluwagbeminiyi Ojedokun

Tojola Yusuf

Aishat Salami

This publication was edited by **Adeboye Adegoke**, Senior Program Manager, Paradigm Initiative

Executive Summary

The Bill is a bold attempt to legislate on digital rights, such as the right to online privacy, anonymity, freedom of expression and opinion online, freedom of information online, right to peaceful assembly and association online.

In 2019, the Digital Rights and Freedom Bill (DRFB) was passed by the National Assembly. However, President Buhari did not sign it into law, citing specific reasons. The Bill is back again to the National Assembly for passage with key changes to its provisions based on the feedback from the President.

The world of technology is rapidly growing and the Bill seeks to enshrine and safeguard the fundamental rights of citizens online, on digital platforms and within the context of emerging technologies.

This research seeks to review the key provisions of the DRFB; how it converges and diverges with relevant existing Laws, Regulations, Frameworks, Guidelines, proposed Bills, and Codes; and proffers solutions where there exist conflicts and overlaps. To achieve that, we reviewed the key provisions of the DRFB and compared it with other legislative instruments.

The Bill is a bold attempt to legislate on digital rights, such as the right to online privacy, anonymity, freedom of expression and opinion online, freedom of information online, right to peaceful assembly and association online,

freedom to learn, protection of privacy of students online, right to create public knowledge, e-governance and financial transparency.

The guarantee of these rights will provide a safe and thriving digital space. Besides, the Bill also covers unique concepts like recognition of digital assets and its inheritability; internet censorship; prohibition of hate speech; content blocking, filtering and moderation; broadband and internet access; intellectual property in public work; and protection of people with disabilities.

While some of these provisions are novel, some are already contained in existing legislative instruments that govern specific issues like communications, fundamental rights, financial institutions, data protection and privacy, consumer protection and other sectors. However, most of these legislative instruments are not all-encompassing to specifically address the uniqueness of the digital space. We identified gaps, possible areas of conflicts, overlaps and made recommendations on how to navigate the murky tide safely.

The research reveals that the Bill diverges with a host of other existing or proposed legislation like the Protection from Internet Falsehood and

Manipulation Bill; Hate Speech (Prohibition) Bill; National Commission for the Prohibition of Hate Speech (Establishment etc.) Bill; Cybercrimes Act; Lawful Interception of Communication Regulation; Nigeria Communications (Enforcement Processes etc.) Regulation; Terrorism Prevention Act and a couple of others addressed later in the research

In the light of these findings, the research, therefore, made useful recommendations around improving the quality of the Bill and advancing advocacy for the adoption of the Bill.



Abbreviations

CBN –	Central Bank of Nigeria
CFRN –	Constitution of the Federal Republic of Nigeria 1999
DPB –	Data Protection Bill 2020
DRFB –	Digital Right & Freedom Bill 2019
ECOWAS –	Economic Community of West African States
ECJ –	ECOWAS Court of Justice
ETB –	Electronic Transaction Bill 2020
FCCPA –	Federal Competition and Consumer Protection Act
FCCPC –	Federal Competition and Consumer Protection Commission
FOIA –	Freedom of Information Act
ICT –	Information Communication Technology
ISO –	International Organisation for Standardisation
IT –	Information Technology
Mbps –	Megabyte per Second
NBC –	Nigeria Broadcasting Commission
NCC –	Nigeria Communications Commission
NDPR –	Nigeria Data Protection Regulation
NHRC –	National Human Rights Commission
NIMC –	Nigeria Identity Management Commission
NITDA –	National Information Technology Development Agency

Introduction

The connectedness of today's world also amplifies the importance of digital rights, making it essential to have them embedded in various legislation and regulations, with their absence spelling catastrophe.

In a world where everyone is digitally connected via daily technological advancements, the proliferation of digital devices and increasing digital platforms, it is cardinal that every individual is capable of understanding and utilising the technological arsenal at their disposal, to ensure the protection of their digital rights from varying attendant risks.

These, among others, are reasons why the importance of the Digital Rights and Freedom Bill in this digital clime cannot be overemphasised.

Digital rights are those rights, human and legal, that an individual should have in order to utilise digital platforms or media fully. They can also be said to be "online fundamental human rights". The connectedness of today's world also amplifies their importance, making it essential to have them embedded in various legislation and regulations, with their absence spelling catastrophe.

The journey to enacting a Digital Right and Freedom Bill in Nigeria started in 2016, and advocacy efforts led to the passing of the Bill by the National Assembly in 2019, which was ultimately denied assent by the President.

The new Digital Rights and Freedom Bill sponsored by Honourable Mohammed Tahir Monguno was introduced to the House, with some fundamental changes based on consultation and stakeholder feedback from organisations like the Nigerian Communications Commission (NCC) and the Federal Ministry of Justice.

The Bill sought "to protect Internet users in Nigeria from infringement of their fundamental freedoms and to guarantee the application of human rights for users of digital platforms or Digital media".

The Bill essentially protects the fundamental rights and freedoms of citizens in the Nigerian digital ecosystem specifying offences concerning acts or omissions contrary to its provisions.

It also prescribes penalties for the offences and provides for the enforcement of citizens' rights, among others.

The National Human Rights Commission (NHRC) is proposed as the body charged with regulating the Bill, and the Federal and State High Courts have original jurisdiction on matters relating to the Bill.

This analysis reviews the Digital Right and Freedom Bill (HB 98) through the prism of other Laws, Codes, Regulations, Guidelines and Bills while considering its importance to the development of the Nigerian digital environment.

It also considers the provisions of the Bill by drawing a parallel to its convergence and divergence with the end goal being to show a lack of conflict between the Bill

and other existing frameworks. In the event of any, our analysis will proceed to proffer recommendations addressing the conflict gaps.



Review of Key Provisions



Right to online privacy

1

Although the Bill prohibits any unlawful interference with an individual's online privacy, the right to online privacy is not explicitly provided for under the Nigerian Constitution. Unlike the right to privacy, which enjoys statutory protection, online privacy is broader than the conception of privacy conceived under the Constitution.

The protection of online privacy has become necessary, with the proliferation of internet-enabled devices, an increase in digital services, and the increased number of internet subscribers. For a long time, there have been concerns about the violation of Nigerians online privacy, and there are reports of the sale of the personal data of Nigerians in an open digital marketplace.

The online privacy right, complements similar existing rights guaranteed under the NDPR, pockets of sector-specific laws and proposed Bills which provide that individuals are entitled to online privacy, and service providers are mandated to strictly protect the privacy rights of users against violation by third parties and the service providers themselves.

The processing of data by third parties is also extensively regulated under the NDPR, with explicit provisions on the rights of data subjects, the use of data processing agreements with third parties, and the obligation to ensure the

security of data. Specifically, data subjects have the rights to lodge complaints under the NDPR to the Supervisory Authority, being NITDA or before the Court.

Surveillance and Interception of Communications

The Bill permits the making of requests for private data following legally stipulated procedures. It also provides that Court warrants will be necessary in order for an intermediary to honour a request for private data, and the request must be reported to the concerned individual . It requires the publishing of the nature and frequency of government requests for personal data.

Besides, the Bill makes it mandatory that disclosure of personal data of private individuals can only be transmitted with a warrant granted by a court of law after the individual has been notified about the disclosure.

This protection is essential to prevent the arbitrary derogation or violation of the right to privacy of a citizen. However, this appears to be subject to the surveillance power of the State, especially when national security, public safety or investigation of crime is cited as a basis.

The power to make such disclosure is subject to a warrant and in some

instances is possible without a warrant at first instance, with the requirement for a warrant applicable after such disclosure.

Unfortunately, it is both common for there to be disregard and a lack of transparency in the procedure for ascertaining the law relied upon by law enforcement agencies.

In a recent case, a citizen was arrested by the Department of State Security (DSS) for tweeting with a parody account in the name of a former president. According to reports, a telecommunication provider disclosed details that enabled the arrest and subsequent detention of the individual, for almost three months without trial.

More recent reports have revealed the purchase of surveillance equipment by the Nigerian Government from an Israeli organisation.

Also, the provision may be whittled down by other laws such as the Mutual Assistance in Criminal Matters Act, which was signed into law in 2016. This Act allows Nigeria to intercept telecommunications and share stored communication or other types of electronic data with third party states as part of a mutual legal assistance arrangement.

the provision may be whittled down by other laws such as the Mutual Assistance in Criminal Matters Act, which was signed into law in 2016

In a recent case, a citizen was arrested by the Department of State Security (DSS) for tweeting with a parody account in the name of a former president.

The data communication sharing is subject to the oversight of the Attorney-General or a Judge.

In stemming the asymmetrical power dynamics between law enforcement and private citizens, the Bill makes it mandatory for private organisations to publish the details of government requests for private citizens' data publicly. This provision strengthens transparency and accountability for the public good. It is an example of global best practices that have been adopted in other climes, which has seen corporations publishing periodic transparency reports.

Statutory Confidentiality

The Bill also imposes the statutory duty of confidentiality. The statutory duty of confidentiality is also contained in the National Health Act, Rules of Professional Conduct for Medical and Dental Practitioners, Medical and Dental Council of Nigeria Act for healthcare professionals, and the Freedom of Information Act. Besides, the Bill confers confidentiality on personal data.

However, statutory confidentiality is not absolute. It can be waived in certain instances, which could be, for instance, where a law expressly provides for it or where the Court decides confidentiality can be waived

Recognition of Digital Asset

The Bill provides for the ownership and management of digital assets of an individual such as passwords, digital contracts, digital receipts, pictures, medical information, bank accounts, writing, or anything else that a user has access to, primarily in the digital space by his heirs or next of kin. Digital assets may also include shopping accounts, file sharing and Peer-Peer accounts, Domain name service accounts, web hosting accounts, affiliate programs, backups, written code, digital currency, or betting accounts .

This provision is the first of its kind in the Nigerian legal space, and its effect is that digital property may now be included in the estate of a deceased person and will by implication, be inheritable. The classification of these items as an asset is a great move, which could also make the asset inheritable.

The extant law on inheritance, the Wills Law and Administration of Estates Laws of different states did not expressly provide that these types of asset can be inheritable. The express provision that it could be inheritable now means that they can be passed on to heirs.

Currently, internet platforms like Twitter, Google and Facebook have legacy policies that could allow people to transfer their accounts to heirs or appoint legacy contacts. The provision will, therefore allow the deceased to live on beyond their death. Though there is no mention of it, nothing in the provision of the extant Wills Law and

Administration of Estate Law applicable in states expressly prohibits digital will or asset.

Section 44 of the CFRN gives every Nigerian citizen the right to acquire and own immovable property anywhere in Nigeria and digital assets, despite having no physical presence, can be transferred from one device to the other, and can therefore be considered as movable property.

Similarly, intellectual property law protects the inclusion of pictures and writings as digital assets and where they are the work of the person, the ownership intersects with the rights of the person under the copyright law especially where it is in electronic form.

On the other hand, the Administration of Estates Laws of different states does not recognise digital assets and have no provisions regarding such. Closely linked to this are the express exclusion of a will, codicil and other testamentary documents from documents that can be digitally or electronically signed.

Thus, the provision of the Bill is an excellent step in the right direction and serves as a wakeup call for an amendment of the Administration of Estates Laws.

Currently, internet platforms like Twitter, Google and Facebook have legacy policies that could allow people to transfer their accounts to heirs or appoint legacy contacts.

Security of Data

The integrity and confidentiality of personal data are two of the information security triad necessitating the creation of appropriate security measures to prevent the risk of deliberately or accidentally compromising personal data intensified through the use of the Internet.

The Bill addresses this through its provision which specifically imposes the obligation to ensure confidentiality and integrity of information. Organisations are mandated to ensure technical and organisational measures to secure information.

The provision is similar to the provision of extant laws like the National Health Act, Cybercrimes Act, national Cloud Policy and other legal instruments, which imposes security obligations on both public and private organisations.

The requirement to publish a privacy notice

Entities that process personal data in the course of their activities are mandated to publish privacy "policies" (notices) that are readily and easily accessible to the public. Similarly, there is a mandatory requirement to publish privacy notices on all digital platforms and when collecting information under the NDPR.

The privacy notice is a fulfilment of the transparency principle and the right of data subjects to be informed. It should

contain information about the processing of personal data being carried out. If the processing involves a child, the notice should be presented in an intelligible and comprehensible manner.

Exceptions to the right to privacy

Rights do not exist in perpetuity and expectedly, the Bill limits the protection of the right to privacy. Under exceptional situations, for instance, in the administration of criminal justice or prevention of crime, the State may limit the right to privacy.

However, such measures shall comply with provisions of the Constitution of the Federal Republic of Nigeria and this Bill, with adequate safeguards against abuse. The guarantees and limitations are quite necessary, primarily because of the need for individuals to have the power to control the reach of their information online. However, the exercise of derogation must be subject to the principles of proportionality and necessity.

Similarly, Section 45 of the CFRN limits the exercise of the right to privacy guaranteed under Section 37 in situations where it is necessary in the interest of defence, public safety, public order, or public health and to protect the rights of others.

The Court of Appeal has also reiterated the curtailing power of Section 45 to the right to privacy. Within the context of online privacy (data protection), the DRFB creates exceptions where the

NDPR will not apply, and this includes the use of personal data in furtherance of national security, public health and safety, investigation of crimes and tax

offences, anonymised data, and household use with no connection to commercial activity.

Recommendations

1

There is a crucial advocacy work to be done to show that the concept of online privacy is distinct and more expansive than the concept of privacy advanced under the CFRN, which offers limited protection.





Anonymity

2

Every person accessing the Internet is entitled to use instruments/technical systems to protect their identity should they wish to remain unidentified. This provision grants the right to access the Internet anonymously and allows a person to prevent the collection of their personal data.

It has become imperative in the country in the face of the clampdown on journalists, human rights activists, protesters and other persons who need to keep their identity anonymous from the State. Anonymity is a survival mechanism which helps whistleblowing efforts and protects marginalised persons and vulnerable populations.

There are reports of the Nigerian Government procuring surveillance tools to spy on its people.

Maintaining anonymity is cardinal to preserving other human rights in the digital space, and crucial to the exercise of civil and political freedom without being subject to discrimination or censorship. The Internet has emerged as a decentralised primary place of refuge for many Nigerians, and it is vital to preserving it as a safe space for users.

It is, therefore, safe to assert that the Internet has evolved to be the modern-day facilitator of free speech and self-determination guaranteed by a perceived expectation of privacy. However, this right may be restricted where it is necessary to safeguard

"public interest, and as necessary, proportional and grounded in law and following the basic features of a democratic society".

A Court may order the identification of an individual where there is a violation of the fundamental rights of another person. The right to remain anonymous on the Internet upsets the dynamics of the balance of rights in the digital space - on the one hand, is the freedom of expression and on the other, the right to privacy, the dignity of the human person and the right to seek legal remedy where appropriate.

However, though there are instances where an individual can hide under the cloak of anonymity to commit crimes, violate the right of others, or cause other civil wrongs such as defamation, it is imperative to maintain a balance. The Nigerian Court can take a cue from the decision in the English case of *Norwich Pharmaceutical Co. vs. Customs and Excise Commissioner*, where the Court held that "an innocent third-party who

"an innocent third-party who has inadvertently facilitated a wrong can be compelled in certain instances to reveal the identity of the wrongdoer, particularly if the wronged party will be precluded from seeking a judicial remedy without the disclosure

has inadvertently facilitated a wrong can be compelled in certain instances to reveal the identity of the wrongdoer, particularly if the wronged party will be precluded from seeking a judicial remedy without the disclosure." The same rationale was upheld in the digital context in the case of *G v. Wikimedia Foundation*, where the Court granted the order to reveal the identity of an internet user that defamed the complainant.

The exceptions allowed under the Clause to lift the veil of anonymity, are consistent with the provisions of Section 45 of the Nigerian Constitution.

Similarly, Article 2.3(1) (i) of the NDPR Implementation Framework creates the exceptions to the material scope of the NDPR, which include the use of personal data in the context of national security and investigation of crime.

It is, however, essential to note that the provision conflicts with the Cybercrimes

(Prohibition, Prevention, Etc.) Act, 2015. While the Bill permits anonymous access to the Internet except where it threatens the public interest, the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 makes it an offence to use any device to avoid detection or prevent identification where there is an intention to commit a crime.

The exception to the right to anonymity under the Bill has goals similar to the Act. However, the wordings of that Clause provide the opportunity for misinterpretation and may, as well, create loopholes.

Similarly, Article 2.3 and 2.4 of the Framework for Public Internet Access mandates Public Internet Access Providers to verify users uniquely and authenticate each user. Mandatory requirement to register for a sim card under the Registration of Telephone Subscriber Regulation negates the concept of anonymity.

Recommendation

1

Clause 4(2) merely states the condition upon which the right of anonymity may be derogated. It is quite nebulous and may give room for unscrupulous interpretations. It is recommended that the condition be more clearly defined, and the determination of the condition be left to the Court only.



Freedom of expression online and the freedom of expression of opinion online

3

The Bill grants the right to freedom of expression online, an extension of the right to freedom of expression guaranteed under the Nigerian Constitution.

Every person is guaranteed the freedom to express and impart information, opinions and ideas of all kinds that can be transmitted to others in any digital form regardless of how controversial the Government may consider it.

The right is not subject to any restrictions, except those which are provided by law and for a legitimate purpose. The safeguard of freedom of expression is one of the hallmarks of a thriving democratic institution. The right to impart knowledge is consistent with Section 39 of CFRN.

Censorship and muzzling of freedom of expression

The censorship and access to information provided by, or about Internet users are prohibited without an order of the Court. It is prohibited to penalise freedom of expression under the guise of protection of national security.

However, there have been recent moves to regulate the use of social media in Nigeria. It includes the express prohibition of the use of intermediaries

to undertake censorship on its behalf or to remove access to content without the leave of the Court.

The State is restrained from unduly restricting, controlling, manipulating and censoring content disseminated via the Internet without any legal basis, justified purpose, or based on broad and ambiguous laws, or in a manner that is unnecessary disproportionate to achieving the intended aim.

According to Google's Transparency Report, between January 2018 - June 2020, the Nigerian Government requested content takedown six times. The Bill outlaws the throttling and jamming of the Internet, or internet shutdown explicitly, and describes it as a confrontation to the freedom of expression.

The Bill notably prohibits the jamming of wireless signals which deprives individuals of their right to expression and information.

Although exceptions exist which may permit censorship, there must be a corresponding lawful basis, which should not be premised on ambiguous law.

The purpose must be justified and there must be recourse to the necessity and proportionality test. On the night of the Lekki shooting, there were accusations against a telecom operator for

throttling the internet connection around Lekki, Oniru and Victoria Island. Protection of freedom of expression is cardinal to the existence of democracy, and any attempt to subvert it is an aberration.

The Bill provides a safeguard in situations where freedom of expression can be waived under the garb of national security, and such derogations must comply with the provision of the Nigerian Constitution.

The Bill frowns at the abusive and inconsistent enforcement of the law to censor public deliberation or create an atmosphere that suppress a free press. The Bill seeks to ensure fairness in perspective and a free press.

Specifically, the Bill prohibits unlawful, unauthorised, and undue restriction on press freedom and thus, conflicts with the revised NBC Code, which has imposed stiffer sanctions, which has been used to sanction media houses.

Freedom of expression online can only be waived where the process is proportionate and necessary in a democratic society. Such restrictions must be defined and provided in an existing law, which must conform to the

The Bill provides a safeguard in situations where freedom of expression can be waived under the garb of national security, and such derogations must comply with the provision of the Nigerian Constitution.

the Bill prohibits unlawful, unauthorised, and undue restriction on press freedom

provisions of the Constitution, concern in the necessity and proportionality test.

The Bill imposes additional safeguards concerning legal frameworks that seek to curtail the freedom of expression. Such a framework must be clear, precise and foreseeable - applied by an independent body that is not arbitrary, effective against abuse and must allow the right to appeal.

The provision of the Bill is consistent with the NCC's Internet Code of practice, which provides that no lawful content software or application shall be blocked or made unavailable to users of internet access.

An Internet Access Service Provider shall not block any lawful content, applications, services, or non-harmful devices, except reasonable network management.

Also, an Internet Access Service Provider shall not impair or degrade lawful internet traffic based on internet content, source, destination, application, or service, or use of a non-harmful device, except for reasonable network management.

An Internet Access Service Provider shall also have measures in place for the immediate blocking of access to child

sexual abuse content, once notified by the Commission.

The provision of the Bill conflicts with the proposed Protection from Internet Falsehood and Manipulation Bill, which will empower the Government to shut down the Internet or block access to social media platforms.

Further, the Bill suggests that anyone who has cause to believe a statement defames them should have recourse to the civil Court, and should not use the state institution or mechanism to perpetuate abuse. It is important to note that criminal defamation also exists under Nigerian law.

Prohibition of hate speech

The right to freedom of expression does not, however, permit hate speech and government concerns about hate speech shall not be abused to discourage citizens from the expression of thoughts and ideas. Similarly, the Cybercrimes Act and the NBC Code address hate speech and sanction it.

The Bill provides that the Government cannot suppress or discourage legitimate views under the guise of regulating hate speech. It also provides sufficient safeguards for addressing and balancing concerns about hate speech by allowing only the Court to be the sole determinant of such issues.

This independent review is laudable and gives credibility to the Process when compared to the current arbitrariness that leaves law enforcement agencies with much room for abuse under both the Prohibition of Hate Speeches and

Other Related Matters Bill (Hate Speech Bill) and the Cybercrimes Act.

Hate Speech, under the Hate Speech Bill and DRFB were defined in similar terms to include all forms of expression or actions that spread, incite, promote or justify religious, ethnic, cultural, or racial hatred, xenophobia, or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrant and people of immigrant origin.

Where such expressions are made to instigate war, civil disorder and violence, a person commits an offence. There could be a potential conflict with the prohibition of hate speech under the Hate Speech Bill, where both are passed into law. The DRFB imposes safeguards when determining what constitutes hate speech, while such an independent review mechanism is absent under the Hate Speech Bill.

Also, life imprisonment or death is the penalty for hate speech under the Hate Speech Bill, if it results in death. The punishment is excessive in comparison to the proposed sanction under the DRFB, which stipulates an imprisonment

The life imprisonment or death punishment in the hate speech bill is excessive in comparison to the proposed sanction under the DRFB. While there may be concerns that the DRFB specifies punishment for hate speech, the bill provision for judicial oversight may help mitigate the likelihood of abuse.

term not less than seven years or a fine not less than five million Naira, or both and compensation for the victim.

Another conflict arises in Bill's provision which guarantees a right to freedom of expression online, and the Cybercrimes Act, which under Section 24(b), prohibits the sending of electronic messages to cause annoyance, inconvenience, danger, obstruction, insult, injury, and criminal intimidation.

The absolute right guaranteed by the Bill is prone to abuse. However, Section 24(b) of the Act may as well be abused by the Government in situations where there is an expression of opinions unfavourable to the Government. Coincidentally, in July 2020, the ECOWAS Court of Justice ruled that by adopting the provisions of Section 24 of Cybercrime (Prohibition, Prevention, etc.) Act, 2015, it violates Articles 9 (2) of the African Charter on Human and Peoples' Rights and 19 (3) of the International Covenant on Civil and Political Rights.

Consequently, it ordered the Nigerian Government to repeal or amend Section 24 of the Cybercrime Act 2015, following its obligation under Article 1 of the African Charter and the International Covenant on Civil and Political Rights.

Another conflict arises in Bill's provision which guarantees a right to freedom of expression online, and the Cybercrimes Act, which under Section 24(b), prohibits the sending of electronic messages to cause annoyance

in July 2020, the ECOWAS Court of Justice ruled that by adopting the provisions of Section 24 of Cybercrime (Prohibition, Prevention, etc.) Act, 2015, it violates Articles 9 (2) of the African Charter on Human and Peoples' Rights and 19 (3) of the International Covenant on Civil and Political Rights.

Content blocking, filtering and moderation

In order to censor or remove access to a copyrightable content, the Government or intermediary must get an order from the Court to do so.

To restrict freedom of expression on the ground of copyright, the Government must demonstrate that it is prescribed by law, in order to protect the ends that copyright seeks to achieve, necessary in a democratic state, with the burden to prove the existence of copyright being on the owner.

The DRFB categorically prohibits disconnection from the Internet on the ground of copyright infringement. It also prohibits the intentional blocking of content by a person without copyright, while giving the victim an entitlement to compensation in a Court of law.

The provision is consistent with the draft Copyright Bill 2015, which gives the Copyright Commission the power to block content directly or with assistance, where the content infringes

copyright. The DRFB permits this, and besides requires compliance with the CFRN, and international human rights laws in doing so.

The draft also permits the conversion of works into readable formats for the visually impaired. Similarly, the Marrakesh Convention creates a copyright exemption for the adaptation of copyright works into a format that is readable for the visually impaired, which is precisely what the DRFB enshrines.

In furtherance of its provision on equal access to education, the Bill

pronounces the lack of an exception for the visually impaired, minority language speakers and persons with low literacy level as a violation of their right to private life, freedom of expression, and freedom to participate in cultural life.

The derogation for the sake of the visually impaired is laudable, especially in light of the Marrakesh Treaty of 2016 which Nigeria ratified in 2017. Another laudable provision is the requirement to comply with the Constitution, the rule of law, and other human rights law to which Nigeria is a party, in filtering, blocking or restriction of access to content including copyright content.

Recommendations

1

The question, then, is what would be legitimate enough to limit the freedom of expression online?

2

There should be more robust advocacy for the adoption of the provision of the DRFB as preferable to the Hate Speech (Prohibition) Bill (HB. 246), 2019 and Section 24 of the Cybercrimes Act. The DRFB is more human right advancing and puts in place human rights-respecting safeguards.

3

Clause 6 (21) limits the right of action of a person who has been defamed to a civil action. This model is more human right respecting compared to criminal defamation that exists under the Criminal Code Act, which has been used as a tool to oppress and suppress dissent. A civil action benefits the complainant more. Besides, the fine paid in a criminal defamation suit goes to the government. We recommend that the civil suit model should be adopted over the criminal approach for defamation.

4

The exception created for low-level literates and minority language speakers is against the whole economic principles in copyrights. One of the essences of copyrights is for the owner to be able to enjoy economic gains from his works. Extending the exceptions to cases as these would mean that within Nigeria, the owner of the work would rarely reap the fruit of his labour. The portion of Nigeria's population that is literate is meagre compared to the illiterates. Also, there are over 500 native languages in Nigeria, of which three are widely-spoken. It means that copyright exceptions will cover the largest part of the population and in the end, deprive the owner of the work of any gains at all.

5

There is a need to separate copyright from other rights. It is important because the principles governing copyright differ from those of other information. Inserting copyrights under every right will only bring about needless litigation and conflicts.



Freedom of information online

4

An individual is guaranteed the right to access the Internet for information gathering, and this right extends to urban poor and rural areas, where the Internet is slow or unaffordable.

The Bill prohibits explicitly or allows restricted access to a specific category of information, such as child porn, hate speech, defamation, direct or public incitement to commit suicide and genocide.

It complements provisions of other laws like the Cybercrimes Act and Internet Code of Practice, which criminalises child pornography and cyberstalking.

Broadband and internet access

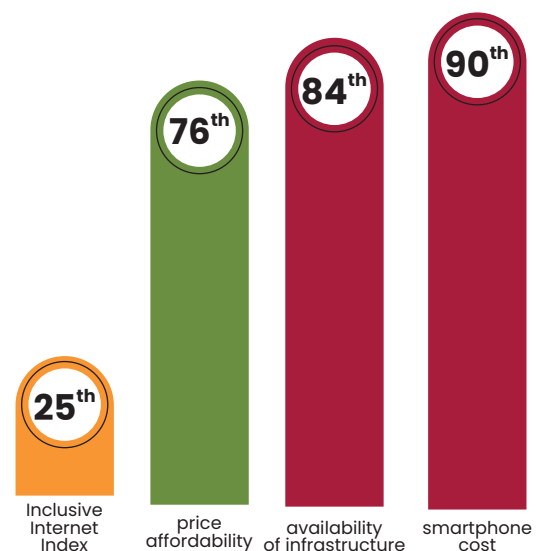
The Bill mandates that broadband access shall be made commonly available as connectivity is crucial for accessing resources, and requires continued focus on competitive broadband access using suitable technologies – wired and wireless, and national collaborative networks.

Nigeria currently ranks 25th in the world on the Inclusive Internet Index. Nigeria ranks 90th on smartphone cost, 76th on price affordability, and 84th on availability of infrastructure. Vast digital divide, access and inclusion are still significant problems in Nigeria, despite the Government's announcement that

the price of internet data crashed. The provision complements the ambitious target set by the Government in the new National Broadband Plan, which seeks to attain cheaper cost for internet data and expansion of broadband penetration.

This provision is laudable considering the importance of broadband penetration to the digital economy and the objective of attaining 70 per cent broadband penetration in 4 years as contained in the National Digital Economy Policy and Strategy. Also, the plan is that there will be broadband connectivity delivering a minimum of 10 Mbps in rural areas and a minimum of 25 Mbps in urban areas to every Nigerian at an affordable price and quality by 2025. It also aims to target 90% of the population.

Nigeria's ranking on broadband and internet access



The provision is consistent with the National Digital Economy Policy and Strategy (2020 – 2030), the 3rd of 8 pillars to accelerate the development of the Nigerian digital economy which requires reliable infrastructure (deployment of fixed and mobile infrastructure to deepen the broadband penetration in the country).

The requirement for open government data

The Bill mandates that Government held data should be made available publicly for free, or after payment has been made, in appropriate circumstances. There should not be barriers to access Government held data.

The provision creates a statutory requirement that will strengthen the open data policy pursued by the Government, which will promote transparency and accountability in governance.

The Bill fails to make a distinction on the type of data. For personal data, it will be subject to the NDPR, DPIF, the Guideline on Public Institution on Processing of Personal Data and the proposed Data Protection Bill 2020. Before processing such data, the lawful basis has to be established. Similarly, some data could be subject to confidentiality rules under the Freedom of Information Act and the Evidence Act.

The Bill mandates that Government held data should be made available publicly for free, or after payment has been made, in appropriate circumstances.

Intellectual property in public work

The Bill provides that copyrightable materials held by public bodies shall be licensed for reuse following extant information access law and licensing framework. The provision is consistent with the Freedom of Information Act.

Similarly, Section 14(2)(b) of the Copyright Act provides that access to the public record of a state, being records for the storage or custody provided in law, does not require authorisation or licensing of the owner of the copyright.

Consequently, there will be no infringement of the copyright in such work by supplying and reproducing it.

Right to access the Internet

The Bill provides the right to use the Internet to access information, share information, conduct business online, and the right to express a personal opinion online. It is also illegal to deny or censor access to the Internet without adequate reasons.

At the height of the fight against terrorism in the North-East region of the country in 2013, the Military shut down telecom infrastructure, which meant internet blackout, an action justified on the grounds of national security. The Clause seeks to prevent a situation where the Internet could be shut down at will.

Protection of people with disability

The Bill provides that persons living with a disability will have the right to access the Internet and should suffer no discrimination. This provision strengthens relevant sections of Discrimination with Persons with Disability (Prohibition) Act 2018, Lagos State Special Peoples Law and Plateau State Handicapped Law, which seeks to protect persons living with a disability. Section 42 of CFRN prohibits discrimination against any person regardless of the circumstance of their birth.

Content blocking and filtering

Blocking and filtering of access to websites or content are expressly prohibited, which includes social media. There have been previous reports of blocking of access to certain websites in the country. According to the political authority in Nigeria, social media was responsible for information disorder



The Bill provides that persons living with a disability will have the right to access the Internet and should suffer no discrimination.

that led to violence and destruction witnessed in the country. In a national address, the President attributed the violence in the country to social media. The reaction was followed by the Minister of Information and Culture urging the House of Representatives to ensure the passage of a law to regulate the use of social media, a comment by the National Security Adviser and a similar debate was held at the Lagos State House of Assembly.

The provision conflicts with the provision of Protection from Internet Falsehood and Manipulation Bill, which seeks to confer the Government with the power to block access to specific platforms.

Recommendations



More advocacy should be done in advancing a case for the adoption of the DRFB as against the provisions under the Protection from Internet Falsehood and Manipulation Bill.



Right to peaceful assembly and association online

5

As Section 40 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) guarantees the right to peaceful assembly and association. Similarly, the Bill guarantees the right to do so online through any platform. This right shall be guaranteed without interference except those which are provided by law and for legitimate purposes. An example of such limitation is one under the Terrorism Prevention Act, which proscribes the assembly and meetings of persons and organisations for terrorism purposes. The safeguard under Section 40 of the CFRN similarly applies.

Protection against monopolies

The DRFB provides for social and economic openness, to support innovation, and guards against monopolies.

Section 76 of the Federal Competition and Consumer Act complements this provision, by empowering the Federal Competition and Consumer Commission with powers to investigate monopolies which exist concerning the production or distribution of goods or services of any description, or to the export of goods or services of any description from Nigeria.

In the instance where a monopoly is found to exist, monopolistic reports from the Commission are referred to a

tribunal which has further power to prohibit or restrict the acquisition transaction, require a person supplying the goods to publish its price list, declare such monopolistic agreement to be unlawful, among others.

These powers of the Commission regarding monopolies, also extends to those arising outside Nigeria, if the undertaking is of Nigerian origin.

These provisions are therefore applaudable for the possibilities they create with providing an equal economic playing ground, which protects against the monopolistic tendencies, capable of stifling small, medium and upcoming business enterprises.

However, this provision may conflict with the exercise of the power of the Federal Competition and Consumer Protection Commission (FCCPC), who may also exercise concurrent jurisdiction with any other regulator. In addition to future conflict, the provision did not specify if the NHRC will share regulatory oversight with the FCCPC or if the regulation will fall under the exclusive powers of the FCCPC.

this provision may conflict with the exercise of the power of the Federal Competition and Consumer Protection Commission (FCCPC), who may also exercise concurrent jurisdiction with any other regulator

Promotion of net-neutrality

The DRFB expressly provides that all data on the Internet shall be treated in an equal and non-discriminatory manner, and shall not be charged differentially, according to user, content, site, platform, application, type of attached equipment, and modes of communication or any other consideration whatsoever.

The provision is similar to Section 3.6 of the Internet Code of Practice, which prohibits discrimination on lawful internet traffic. Net neutrality is the principle that all electronic communications passing through a network are treated equally, independent of the nature of the content, application, service, device, sender address or receiver address.

According to the logic of net-neutrality, any discriminating, blocking or throttling of content or applications requires a regulatory response, in order to prevent such behaviour going forward. Thus, Clause 8(5) of the DRFB is laudable.

The Nigeria Communication Commission (NCC) in 2017 issued the draft code for the Establishment of Internet Industry Code of Practice in support of Net Neutrality. The provision of the DRFB on net-neutrality is consistent with the draft Code and would strengthen the digital space.

The draft Code similarly mandates that all internet traffic be treated equally without discriminating against content,

application or equipment. However, the draft Code imposes limitations where there could be "acceptable traffic management practices" to preserve the integrity and security of the network or service, prevent or mitigate network congestion, provided that equivalent categories of traffic are treated equally.

The provision of Clause 8(5) of the Bill, however, diverges with the provision of the Internet Code of Practice which permits zero-rating so long as it furthers the objective of the NCC Act,

Policy objectives of universal access contained in the National information and communications technology policy of 2012 and the Nigerian ICT Roadmap.

Prohibition of discrimination against marginalised people

The Bill recognises the need for inclusion and full integration of all persons, by providing substantive equality for marginalised peoples or groups.

The provision is in general consonance with several laws, such as Section 42 of the 1999 constitution which provides that a citizen shall not be discriminated upon because of their ethnic group, place of origin, sex, religion or political opinion.

Section 17 of the Constitution, though not justiciable, also provides that the State shall direct its policy towards ensuring that all citizens can secure adequate means of livelihood, as well

as suitable employment and that there should be equal pay for equal work without discrimination on the grounds of sex or any other ground, without discrimination on any group whatsoever.

Further to this, the Discrimination against Persons with Disabilities (Prohibition) Act also reiterates the need for inclusion and full integration of persons with disabilities in society. It provides for the prohibition of discrimination of a person on the ground of disability by any person or institution and prescribes penalties for its occurrence.

The HIV and Aids Anti-Discrimination Act also complements this provision by reiterating constitutional fundamental human rights for people living with, or affected by HIV or AIDS, and eliminating related discriminations in all settings.

The inclusion of the provision for equality of marginalised people is, therefore, a step in the right direction towards ensuring eradication of discrimination which marginalised people may face from the populace while strengthening the inclusion, equal participation, and general acceptance of all in the society.

Recommendations

1

A rewording of the Clause of the Bill or addition is necessary to provide the instances where an individual may not have the right to assemble for the sake of public and national interest freely. It should be done in a way that prevents abuse by both citizens and the Government alike.

2

The Clause on net-neutrality is silent on zero-rating, which is currently recognised under the Internet Code of Practice. We recommend that the Bill should make regulation about cautiously adopting zero-rating

3

The Bill should guide how it intends to share regulatory oversight with other sector or subject-specific regulators. For example, the provision on monopoly sits exclusively with the FCCPC. It is essential to avoid duplication of regulatory function and friction between regulators, which in turn create chaos for organisations and citizens.



Freedom to learn

6

The Bill has made it mandatory to include internet literacy skills, as well as media and information programmes in school curricula.

The attempt to codify internet literacy into education curriculum is laudable and could propel an increase in the number of young skilled professionals.

Support should also be given to similar learning modules outside of schools. Every individual in Nigeria, adult or child, is guaranteed the freedom to learn. It includes learning how to protect themselves against harmful content while explaining the potential consequences of revealing private information on the Internet.

Learning shall be affordable and available, offered in various formats, to students located in a specific place and students working remotely.

The requirement of affordability is much more realistic than the educational objective in Chapter two of the CFRN

that provides for free education at all stages.

The Bill takes into consideration the realities of governance in Nigeria. This right to learn must also be accorded to persons with disabilities and the Government, at all levels, and is tasked with this responsibility.

The lack of copyright exceptions benefiting people with sensory impairments constitutes a breach of their rights to freedom of expression, private life and their right to participate in cultural life.

Part of the module is expected to address online harm, digital safety, and information disorder. There is also provision mandating the dissemination of knowledge in the minority language. It will prevent marginalisation, discrimination and forceful learning of a majority language by persons from the minority. Equal access to knowledge by people of all languages and levels of literacy should also be promoted



Part of the module is expected to address online harm, digital safety, and information disorder. There is also provision mandating the dissemination of knowledge in the minority language



Protection of privacy of students and learners

7

The Bill ensures the protection of student's privacy, both offline and online, is an inalienable right.

This provision is strengthened by Section 37 of the CFRN that guarantees the right to privacy for all citizens. Similarly, in the online context, the NDPR confers data protection rights.

Students are confronted with increasing privacy risk in the digital space, some of which are, the use of stalkerware for mass surveillance, absence or lack of comprehensive privacy notice, remote learning and surveillance, the risk with the use of cloud, excessive data collection, lack of transparency with retention period, the commodification of students data, unfair penalisation of students who do not have control over their environment (less functional hardware or low-speed Internet), lack of sufficient or appropriate security and the intersection with the use of social media. Consequently, it has become critical to extending protection to students.

There is a need to address the right to privacy of students. It is imperative because of various privacy violation prevalent in Nigerian schools which may extend to their parents, as schools collect parents' information as it was the case of an elementary school in Lekki, Lagos state which disposed of its old personal computers without wiping out all information on the computers.

Subsequently, parents began complaining about a series of unusual requests from the school which the latter had not sent.

Also, students in primary and secondary schools and a few in tertiary institutions are mostly minors who require superior protection in the processing of their information. In June 2020, websites of some schools were hacked in Nigeria, giving hackers access to information which was shared on a platform created for the same purpose.

Mandatory requirement to display a privacy notice

Similar to Clause 3 of DRFB, the Bill makes it mandatory for educational institutions to display a privacy notice containing their privacy practices and their processing activities to students. These include details of personal information to be processed and third parties it will be shared with.

Further, the notice is also expected to explain the privacy implications of their processing to the students. It has become cogent with the rise of Massive Online Open Courses (MOOC), Learning Management Software (LMS) and other online mediums in the wake of the outbreak of the coronavirus.

These provisions complement the existing Article 2.5 of the NDPR that similarly mandates the display of

privacy notices. It is a step in the right direction as no legislation in Nigeria mainly caters for the privacy rights of students, more so, online.

Service providers are mandated to make clear to students the implications of their choice to make their information available for collection and use.

The service provider must communicate any changes in terms of service and privacy notice.

Intellectual property right in work created

The Bill confers intellectual property rights on online students for work they create. Mainly, the copyright vested by the Copyright Act to an individual or body corporate under nationality or domicile, or by reference to the country

of origin, is vested initially in the author of the work.

However, schools and LMSes could have variegated intellectual property terms and conditions.

Clause 10(8) presupposes a term of privacy as a contract between the provider and the student, which negates the spirit of what a standard privacy notice is under the NDPR.

The NDPR provides that the organisations shall display a simple and conspicuous privacy notice, as against a term of privacy which requires a form of consent. A privacy policy is merely an information statement informing the public about processing activities.

Recommendations

1

The provisions titled privacy of students and learners are not limited to the right to privacy, it covers the right to learn, own intellectual property, online system financial health knowhow, fair, transparent financial accounting, and so on. It is recommended that it is titled Digital Rights of Students or something along the line of particular provisions or protection for students

2

The Bill does not address situations where the students in question are minors. Can they exercise those rights on their own or require parental or guardian participation? If not, who can? It puts into consideration the very many risks of online presence, including privacy. Though, the DPIF specifies the age of a child to be any person less than 13.

3

The provision of Clause 10 (10) of the Bill is somewhat unclear as it did not relate the financial accounting to the student's online learning. We recommend it is placed under the appropriate heading.



Students are confronted with increasing privacy risk in the digital space, some of which are, the use of stalkerware for mass surveillance





Right to create public knowledge

8

Where a provider promises to issue a certificate, badge or credential, the authenticity and relevance must be explained and established clearly. It also provides for the promotion of research capacity. It appropriates human resource development in the field of ICT skills with a view to, among other things, promote digital literacy,

ICT for education, and the development of specialist or expert capacity in ICT. It also advocates for the integration of ICT into learning and teaching and to enhance teachers' capacity in IT. The Bill mandates access to learning materials and collaboration at an affordable rate, including broadband access.

Recommendation

1

The Bill's provisions on creating public knowledge appear to be merely an unenforceable suggestion. It appears so similar to the provisions of Chapter 2 of the Constitution, which is not justiciable. We recommend it is drafted as a mandatory obligation.

2

We recommend that the Bill should make it a mandatory requirement to conduct a Human Right Impact Assessment before launching a digital identity program by both public and private institutions. The copy of the impact assessment should be made available publicly or should be provided from those who request for it. The assessment should extend to any processing that involves biometric and genetic data of individuals.

3

The practicability of Clause 11 as a whole in Nigeria may take much time to be seen as only about 46% of the population is connected to the Internet, and many schools are yet to adopt the use of IT by their inability to afford it.



E-governance and financial transparency 9

The Bill provides for an open and modernised self-governance system which guarantees free flow and access to information by both citizens and Government which should encourage interactions on both ends consistent with the country's E-Government Masterplan.

An increasing number of government agencies are digitising services, and while some have been effective, some have been problematic, while some have refused to adopt digitisation.

The Government is encouraged to use social media to its democratic advantage as all over the world, more governments are using social media to connect with their citizens. This provision

is consistent with the Framework and Guideline for the Use of Social Media in Public Institutions.

The Government is also mandated to pursue a national identity program built on accuracy, effectiveness and efficiency, which incorporates technology that reduces digital identity theft and fraud.

This provision is consistent with the provision of the National Identity Management Commission Act overseen by the NIMC, the government agency responsible for maintaining the country's national identity program. Nigeria's foundational identity program is in the pipeline.

Recommendation

1

The provision is silent on the obligation to ensure the security of e-governance platforms. Government agencies are known to be weak in the area of digital security. More recently, some government websites were defaced or suffered data breaches.

2

The structure of the Clauses should be consistent. An example being Sub-clause 9, which is repeated twice for two specific provisions.



General Recommendations



1

There is a need to separate copyright from other rights. It is necessary because the principles governing copyright differ from those of other information. Inserting copyrights under every right will only bring about needless litigation and conflicts



2

The exclusion of name, title, business address or telephone number of an employee of an organisation from personal information is restrictive. It exposes the employees to undue risk to their privacy and data protection rights. They have a right to determine what happens to such data collected from them.



3

Clause 3(6) and (7) of the Bill can be merged into one to avoid unnecessary repetition. The right to confidentiality and integrity of data can be contained in just one Clause. In the same light, Clause 6(1) and (4) of the Bill are practically the same and can be listed under one heading.



4

The provisions of Clause 6(9), (10), (11), (12) all border on the conditions for restriction of the freedom of expression online. They can all be merged into two sub-clauses to avoid unnecessary repetition.



5

Some of the issues considered topical subjects within the scope of the law might be outside the statutory power and competence of the National Human Right Council (NHRC). For example, the issue of monopoly falls within the exclusive remit of the FCCPC.



6

It is important to use terms consistently, to avoid confusion and contextual chaos. Words, when misused could get lost in context. For example, Clause 3(2) of the Bill creates the statutory duty of confidentiality, while Clause 3(6) & (7) refers to confidentiality in the context of security of data. Clause 3 (9) creates the obligation to have "data privacy policy", when in actual fact it meant a privacy notice. Clauses 3 (6), 3 (7) and 10 (2) of the Bill are in clear reference to data protection, considering the Bill does not intend to duplicate the provision of existing laws, this will need to be revised. Use of the "data subject" still have reference to data protection and it can be replaced with "individuals". Similarly, use of "personal data" could be replaced with "personal information".



7

Besides, the provisions can be grouped under appropriate headings, which will fit the context they should exist, rather than have different provisions in unrelated pockets. For example, the Clause on right to online privacy also covers recognition of digital asset. Similarly, the Clause on peaceful assembly covered protection against monopolies.



8

It is a great idea to create complementary provisions to strengthen existing legal frameworks. However, co-regulation could lead to over-regulation. Existing regulators are likely to protect their sectoral base jealously. It may also create additional compliance obligations for organisations. We recommend allowing a robust inter-agency collaboration. For example, there are Clauses that caters for domain-specific subjects like monopoly and identity management which would be considered under the regulatory purview of FCCPC and NIMC respectively, without defining the regulator, it could create multiple regulatory compliance obligation on organisations.



9

No existing legal instrument available in the country currently addresses online harm as much as the DRFB. However, the DRFB could as well advance that by having additional provisions to regulate online harms.



10

The Bill should specifically outlaw backdoor encryption in Nigeria. In addition, decryption of data should be done after getting an order of the Court. Currently, the Cybercrimes Act requires an order of the Court for decryption, in contrast, the Lawful Interception of Communication Regulation does not impose any safeguard or require the order of a Court. Unfettered decryption power in the hands of law enforcement agents threatens human rights.



11

Though, the President has said the previous version of the Bill duplicates existing or proposed laws, it is our submission that there is no inherent problem where a law complements an existing law, especially when it strengthens the effective administration and offers clarity, which is what the DRFB has done largely.



Conclusion

The research has highlighted the importance of digital rights as an extension of human rights guaranteed under different laws. The research has demonstrated the limitations of some of the extant legislation in protecting people in a digital context. Digital rights are human rights, and it has become crucial to legislate on them.

The research has carefully shown the convergence and divergence of the Digital Rights and Freedom Bill with other extant and proposed legislations. At the same time, it is critical to the preservation of our digital space and is to keep the advocacy and conversation going till the Digital Rights and Freedom Bill becomes a law.

ANNEXURE I

List of Laws, Guidelines, Frameworks, Bills and Regulations

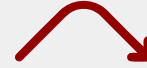
1. Administration of Estate Law of Lagos State
2. CBN Consumer Protection Regulation, 2016
3. CBN Cybersecurity Risk-Based Framework for Deposit Money Banks and Payment Service Providers, 2018
4. Central Bank of Nigeria Consumer Protection Regulation
5. Credit Reporting Act, 2017
6. Criminal Code Act, Cap C39, Laws of the Federation of Nigeria, 2004
7. Data Protection Bill 2020
8. Digital Right & Freedom Bill 2019
9. Discrimination against Persons with Disabilities (Prohibition) Act 2018
10. Electronic Transaction Bill 2020
11. Evidence Act, 2011
12. Federal Competition and Consumer Protection Act, 2019
13. Freedom of Information Act, 2011
14. International Organisation for Standardisation
15. Lawful Interception of Communication Regulation, 2019
16. Mutual Assistance in Criminal Matters Act 2016
17. National Digital Economy Policy and Strategy (2020 - 2030)
18. National Identity Management Commission Act, 2007
19. NCC Internet Code of Practice, 2019
20. Nigeria Broadcasting Commission Code
21. Nigeria Communications (Enforcement process etc.) Regulation 2019
22. Nigeria Communications Commission Act, 2003
23. Nigeria Data Protection Regulation Implementation Framework, 2020
24. Nigeria Data Protection Regulation, 2019
25. NITDA Framework for the Use of Social Media in Public Institutions, 2019
26. Registration of Telephone Subscribers Regulation, 2011
27. Telecommunications Facilities (Lawful Interception of Information) Bill, 2019 (HB 42)
28. Terrorism (Prevention) Act, 2011
29. The Constitution of the Federal Republic of Nigeria, 1999 (As Amended)
30. The Copyright Act, Cap C28, LFN 2004
31. The Draft Code for the Establishment of Internet Industry Code of Practice in Support of Net Neutrality (the Draft Code)
32. The Draft Copyright Bill, 2015
33. The Marrakesh Treaty, 2016
34. The Nigerian National Broadband plan, 2020 - 2025
35. Wills Laws of Various States

ANNEXURE I

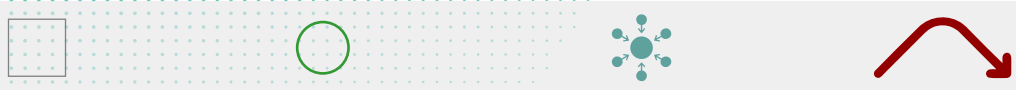
COMPARISON OF DRFB WITH OTHER REGULATORY FRAMEWORKS CHART

The table represents the intersection and divergence of various parts of the Digital Rights and Freedom Bill with other legal frameworks. The legal framework considered include extant laws, proposed Bills, regulations, and guidelines made by the Federal or States Government or their ministries, departments or agencies. The objective is to show the DRFB does not conflict with any extant law.

Value	Digital Rights and Freedom Bill	Convergence (Similar Provision in other laws)	Divergence (conflict with other laws)
Freedom of expression Online	Yes Clause 7(9) and 8(1)	Section 39 of CFRN	Protection from Internet Falsehood and Manipulation Bill Cybercrime Act
Prohibition of Censorship	Yes Clause 6(5), (17) - (19); 7(4)	Internet of Code of Practice	Protection from Internet Falsehood and Manipulation Bill
Protection of persons with disability	Yes 7(6), (7), & 9 (9)	Discrimination Against Persons Living with Disability (Prohibition) Act Plateau State Handicapped Law Lagos State Special People's Law Section 42 of the CFRN	
Blocking and filtering of content	Yes Clause 6(12)(e) - (g); 7(9)	Internet of Code of Practice	Protection from Internet Falsehood and Manipulation Bill



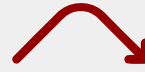
Value	Digital Rights and Freedom Bill	Convergence (Similar Provision in other laws)	Divergence (conflict with other laws)
Online privacy for individuals	Yes Clause 3(6)(7)	NDPR; NDPR Implementation Framework - Article 3.2(6); CBN Consumer Protection Regulations - Article 5.4; Credit Reporting Act - Section 9(1); National Health Act - Section 28; Section 9 - Guidelines for the Provision of Internet Service; Section 19(3) - Cybercrimes Act; Part IV - Electronic Transaction Bill; Section 1 - Draft Data Protection Bill; Part VI - General Consumer Code	
Obligation to ensure the security of information	Yes Clause 3(5),	NDPR - Article 2.1(1)(d), 2.6; NDPR Implementation Framework - Article 3.2(6); CBN Consumer Protection Regulations - Article 5.4.1; Electronic Transaction Bill - Section 23; Draft Data Protection Bill - Clause 3(1)(g); General Consumer Code - Section 43(1)(g)	



Value	Digital Rights and Freedom Bill	Convergence (Similar Provision in other laws)	Divergence (conflict with other laws)
Obligation to publish privacy notice	Yes Clause 3(9)	NDPR - Article 2. 5; NDPR Implementation Framework - Article 3.2(iii), (iv)	
Prohibition of hate speech	Yes, with judicial oversight Clause 6(13) - (15)		Hate Speech (Prohibition) Bill - Section 2; National Commission for the Prohibition of Hate Speech (Est. etc.) Bill - Section 4 Cybercrimes Act - Section 24
Digital copyright	Yes Clause 3(3), 10(6)	Copyright Act	
Role of Court in determining hate speech	Yes Clause 6(16)		
Prohibition of suppression of media and freedom of expression	Yes Clause 7(10)	Section 39 of the CFRN	Hate Speech (Prohibition) Bill - Clause 2; National Commission for the Prohibition of Hate Speech (Est. etc.) Bill - Clause 4; NBC Code
The statutory obligation to ensure confidentiality	Yes Clause 3(2), (6) and (7)	CBN Consumer Protection Regulations - Article 5.4.1; Credit Reporting Act - Section 9(1); National Health Act - Section 26(1)	



Value	Digital Rights and Freedom Bill	Convergence (Similar Provision in other laws)	Divergence (conflict with other laws)
Net neutrality	Yes Clause 8(5)	Internet Code of Practice Draft Code for the Establishment of Internet Industry Code of Practice 2017	
Permits surveillance with democratic safeguards	Yes Clause 3(8)	Nigeria Communications (Enforcement Process etc.) Regulation 2019 - Section 8 (2) (a) Cybercrimes Act - Section 38 (4) Section 4, 7, 8, 10 - Lawful Interception of Communications Regulations; Section 13 - Terrorism (Prevention) (Amendment) Act; Section 39 - Cybercrimes Act; NDPR Implementation Framework - Article 10.1.1	Section 12 - Cybercrimes Act Lawful Intercept ion of Communication Regulation Nigeria Communications (Enforcement process etc.) Regulation - Section 8 (2)(b) Terrorism Prevention Act - Section 25 Telecommunication s Facilities (Lawful Interception of Information) Bill, 2019 (HB 42)
Preservation of freedom of expression	Yes Clause 5 and 6	Section 39 - CFRN	Cybercrimes Act - Section 24(b); Hate Speech (Prohibition) Bill - Clause 2; National Commission for the Prohibition of Hate Speech (Est. etc.) Bill - Section 4



Value	Digital Rights and Freedom Bill	Convergence (Similar Provision in other laws)	Divergence (conflict with other laws)
Protection of privacy	Yes Clause 3(1), 3(5), and 10(1)	Section 37 - CFRN; Article 2.9 - NDPR; Section 2(e) - Lawful Interception of Communications Regulations; Article 5.4.1 - CBN Consumer Protection Regulations; Section 1(b), 9(1) - Credit Reporting Act; Section 8 - Child Rights Act; Lagos State Tort Law	Section 4, 7, 8, 10 - Lawful Interception of Communications Regulations; Section 8 - Nigeria Communications (Enforcement Process, Etc.) Regulations; Section 13 - Terrorism (Prevention) (Amendment) Act

References

- ParadigmHQ, “Where We Are: A Kaleidoscopic View of Digital Rights in Africa - Paradigm Initiative” (Paradigm Initiative, April 10, 2017) <<https://paradigmhq.org/tomiwa-digirights-africa/>> accessed December 14, 2020
- Digital Rights and Freedom Bill 2016 (HB490) (Placbillstrack.org, 2019) <<https://placbillstrack.org/view.php?getid=1801>> accessed December 14, 2020
- “Buhari Declines Assent to Digital Rights and Freedom Bill, Four Others | The Guardian Nigeria News - Nigeria and World News” (The Guardian Nigeria News - Nigeria and World News, March 20, 2019) <<https://guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/>> accessed December 14, 2020
- Udoka Chiefe, “Your Online Freedom Is at Risk; the New Digital Rights and Freedoms Bill May Just Save It” (Techpoint Africa, December 3, 2019) <<https://techpoint.africa/2019/12/03/digital-rights-freedoms-bill/>> accessed December 14, 2020
- Explanatory Memorandum, Digital Rights and Freedom Bill 2019
- Clause 15 DRFB
- Clause 3 of the DRFB.
- Clause 3(1) ibid
- Section 37 of CFRN
- Nigeria has estimated over 120 million active internet connected lines, though, the number does not reflect the number of unique users. “Africa Internet Users, 2020 Population and Facebook Statistics” (Internetworldstats.com, 2020) <<https://www.internetworldstats.com/stats1.htm>> accessed December 13, 2020
- Cybersecfill, “Data Hawking and the Economics of Perversion” (CybersecFill, November 6, 2020) <<https://web.archive.org/web/20201106191241/https://www.cybersecfill.com/data-hawking-and-economics-of-perversion-2/>> accessed December 13, 2020
- Nigeria Data Protection Regulation. It was released by the National Information Technology Development Agency (NITDA) in January 2019. As a Regulation, it is not considered to have the same strength as an Act of the National Assembly. The enforcement of the Regulation has been questioned. Adegoke A, “DIGITAL RIGHTS AND PRIVACY IN NIGERIA” <https://ng.boell.org/sites/default/files/2020-08/Digital%20Rights%20and%20Privacy%20in%20Nigeria_0.pdf> accessed December 14, 2020
- Credit Reporting Act, National Health Act, CBN Consumer Protection Regulation etc. are examples of sector-specific frameworks.
- Data Protection Bill 2020, Electronic Transaction Bill, CBN Data Protection Regulation are examples of pending legislation that specifically provides for data protection rights.

- Clause 3 (5) of DRFB
- Article 3.1 of the NDPR
- Article 2.7 of the NDPR
- Article 2.6 of the NDPR
- Article 4.1 (1) of the NDPR
- Article 3(8) of the NDPR
- Article 3(9) of the NDPR
- Clause 3 (8) of DRFB
- Section 7 (3) of the Lawful Interception of Communication Regulation. See the Nigerian Chapter Schmidt C, "European Essential Guarantees Guide – A Global Look at Fundamental Rights to Privacy & Data Protection" (Essentialguarantees.com, 2020) <<https://www.essentialguarantees.com/>> accessed December 13, 2020
- Section 8 (2) (b) of the Nigeria Communications (Enforcement Process etc.) Regulation 2019 mandates telecommunication companies to provide basic information to law enforcement agents that presents a written request if duly signed by a police officer not below the rank of ASP. This could be abused. Section 7 & 8 of the Lawful Interception of Communication Regulation permits the interception of communications in situations as provided by the Regulations with or without warrant. See also Section 38 (4) of the Cybercrime (Prohibition, Prevention, etc.) Act 2015.
- Section 8 (2) (a) of the Nigeria Communications (Enforcement Process etc.) Regulation 2019 mandates telecommunication companies to provide basic information only when there is a valid court order
- A warrant is required after 48 hours. Section 12 (4) of the Lawful Interception of Communication Regulation, Section 25 (1) of Terrorism Prevention Act
- Law enforcement agencies are known to use telecom companies to conduct surveillance on journalists arbitrarily. Rozen/CPJ J, "How Nigeria's Police Used Telecom Surveillance to Lure and Arrest Journalists – Committee to Protect Journalists" (Committee to Protect Journalists, February 13, 2020) <<https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/>> accessed December 13, 2020
- "I Spent 82 Days in Detention – Student Who Created Jonathan's Parody Account" (Punch Newspapers, August 12, 2020) <<https://punchng.com/i-spent-82-days-in-detention-student-who-created-jonathans-parody-account/>> accessed December 13, 2020
- Karombo T, 'More African Countries Are Relying on an Israeli Surveillance Tool to Snoop on Private Citizens' (Quartz Africa) <<https://qz.com/africa/1940897/nigeria-kenya-use-israeli-surveillance-tool-to-listen-to-calls/>> accessed 14 December 2020

- To fully understand the surveillance capacity of the Nigerian government, you only need to look at the annual budget in the past 10 years.
 - Part V of Mutual Assistance in Criminal Matters Act 2016
 - Clause 3 (9) of DRFB
 - For example, Google published the number of times the Nigerian government requested user information between 2009–2019. “Google Transparency Report” (Google.com, 2020) <https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:NG&user_data_produced=authority:NG;series=compliance&lu=user_data_produced> accessed December 13, 2020
 - Clause 3 (2) of DRFB
 - Section 26 of the National Health Act
 - Section 44 of the Rules of Professional Conduct for Medical and Dental Practitioners
 - Clause 3 (6) of the DRFB
 - Section 187–196 of the Evidence Act 2011 excludes some communication and Section 14 of the Freedom of Information Act has similar provision.
 - Sainato M, “Facebook and Twitter Are Changing How We Die” (Observer, April 13, 2017) <<https://observer.com/2017/04/twitter-facebook-memorialize-option-remember-deceased/>> accessed December 13, 2020
 - “What Will Happen to My Facebook Account If I Pass Away? | Facebook Help Centre | Facebook” (Facebook.com, 2020) <https://web.facebook.com/help/103897939701143?_rdc=1&_rdr> accessed December 13, 2020
 - Section 43 of the Constitution of the Federal Republic of Nigeria
 - The Copyright Act, Cap C28, LFN 2004
 - Section 17(2)(a) of the Cybercrimes (Prevention, Prohibition, etc.) Act
 - ‘Confidentiality, Integrity, & Availability: Basics of Information Security’ (Smart Eye Technology, 5 October 2020) <<https://smarte yetechnology.com/confidentiality-integrity-availability-basics-of-information-security/>> accessed 14 December 2020
 - Section 38 (5) of the Cybercrimes Act, Section 2.6 of CBN Consumer Protection Regulation, CBN Cybersecurity Risk Based Framework for Deposit Money Banks and Payment Service Providers, Section 2.3.1.9 of the Framework for the Use of Social Media in Public Institutions, Section 3 (6), (7) & 26 of the NIMC Act, Section 9 & 10 of NCC Act, Section 9.2 of Registration of Telephone Subscribers Regulations, 2011, National Cloud Policy, National Cybersecurity Policy, and National Cybersecurity Strategy.
 - Clause 3 (9) of the DRFB
 - There is a distinction between a privacy notice and a privacy policy. While a privacy notice is external facing, a privacy policy is internal facing for an organisation.
- Clause 3(9) of the DRFB

- Article 2.5 of the NDPR
- Article 3.1 (7) of the NDPR
- A child is defined to be a person below the age of 13 and the consent of the guardian or parent will be required to process their data. Article 5.5 of the DPIF
- Article 3.1. (1) of the NDPR
- Clause 3(10) of DRFB
- Clause 3 (11) of the DRFB
- HASSAN v. EFCC (2014) 1 NWLR (PT. 1389) 607 @625 – 626 PARAS. B –D
- Article 2.3 of the DPIF
- Gellert R and Gutwirth S, “The Legal Construction of Privacy and Data Protection” (2013) 29 Computer Law & Security Review 522
<<https://www.sciencedirect.com/science/article/abs/pii/S0267364913001325>> accessed December 14, 2020
- Clause 4(1) of the DRFB
- “Nigerian Journalist Jailed for Refusing to Reveal Source – Committee to Protect Journalists” (Committee to Protect Journalists, August 16, 2018)
<<https://cpj.org/2018/08/nigerian-journalist-jailed-for-refusing-to-reveal/>> accessed December 11, 2020
- “Nigerian Intelligence Bought Tool to Spy on Citizens: Report” (Aljazeera.com, December 8, 2020) <<https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report>> accessed December 21, 2020
- African Academic Network on Internet Policy, “Navigating the Tide of Anonymity Online: Building a Responsible Use of the Internet” (African Academic Network on Internet Policy – AANoIP, July 22, 2019) <<https://aanoip.org/navigating-the-tide-of-anonymity-online-building-a-responsible-use-of-the-internet/>> accessed December 11, 2020
- Clause 4(2) of the DRFB
- This is consistent with the provision of Section 45 of the 1999 Constitution of the Federal Republic of Nigeria, LFN 2004 [1974] AC 133
- “G & Anor v Wikimedia Foundation Inc. | [2009] EWHC 3148 (QB) | England and Wales High Court (Queen's Bench Division) | Judgment | Law | CaseMine” (Casemine.com, 2010) <<https://www.casemine.com/judgement/uk/5a8ff72560d03e7f57ea8998>> accessed December 11, 2020
- Section 11 (1) of the Registration of Telephone Subscribers Regulation.
- Section 39 of the 1999 Constitution of the Federal Republic of Nigeria, LFN 2004
- Clause 6 (5) of DRFB
- Under the current dispensation, the House of Representative have presented two Bills aimed at regulating the use of social media.

- Clauses 6(19) and 7(4) DRFB
- “Google Transparency Report” (Google.com, 2020) <https://transparencyreport.google.com/government-removals/by-country/NG?country_item_amount=group_by:reasons;period;;authority:NG&lu=country_item_amount> accessed December 14, 2020
- Similarly, there were reports that the website of Feminist.co, one of the supporters of the #EndSars protest was blocked from being accessed. “EndSars Promoters FeministCo Website Inaccessible without VPN in Nigeria | The Guardian Nigeria News - Nigeria and World News” (The Guardian Nigeria News - Nigeria and World News, November 26, 2020) <<https://guardian.ng/news/endsars-promoters-feministco-website-inaccessible-without-vpn-in-nigeria/>> accessed December 14, 2020
- Clause 7 (4) of DRFB
- The provisions on censorship have become expedient owing to the trend of internet censorship within Africa. BBC reported that Ethiopia imposed internet shut down for about a month; Tanzania shut down the internet during its general election; Zimbabwe, Togo, Burundi, Chad, Mali and Guinea have at one time or the other shut down their internet. 'Africa Internet: Where and How Are Governments Blocking It?' BBC News (2 November 2020) <<https://www.bbc.com/news/world-africa-47734843>> accessed 14 December 2020
- Clause 6 (17) of DRFB
- Clause 6 (19) of DRFB
- Hillary Essien, “MTN under fire for switching off internet during Lekki Massacre” Peoples Gazette MTN under fire for switching off Internet during #LekkiMassacre (peoplesgazette.com) <<https://peoplesgazette.com/mtn-under-fire-for-switching-off-internet-during-lekkimassacre/>> accessed on 12th December, 2020
- Clause 6 (9) of the DRFB
- Online publishers such as Premium were victims of DDoS (Distributed Denial of Service) attacks believed to be initiated by the government. Emmanuel O, “How PREMIUM TIMES Survived Massive Cyber Attacks during Presidential Election Coverage” (Premium Times Nigeria, April 5, 2015) <<https://www.premiumtimesng.com/investigationspecial-reports/180612-how-premium-times-survived-massive-cyber-attacks-during-presidential-election-coverage.html>> accessed December 14, 2020
- Clause 6 (8) of DRFB
- During the recently concluded #EndSars protest, the Nigeria government was quick to praise the BBC and disparage CNN. Ukpe W, “#EndSARS: BBC Has Reported Extensively on All Sides of This Story – Presidency” (Nairametrics, December 12, 2020)

<<https://nairametrics.com/2020/12/12/endsars-bbc-has-reported-extensively-on-all-sides-of-this-story-presidency/>> accessed December 14, 2020

- Clause 7 (10) of DRFB
- The Code increased the penalty from N500,000 to N5,000,000 for hate speech. Article 3.1.1. Of NBC Code.
- Arise Tv, Channels TV and AIT were sanctioned for their coverage of the protest. “NBC Fines Arise TV, AIT and Channels TV Over #ENDSARS Protest Coverage” (NBC Fines Arise TV, AIT and Channels TV Over #ENDSARS Protest Coverage, 2019)
<<https://www.proshareng.com/news/Products---Services/NBC-Fines-Arise-TV,-AIT-and-Channels-TV-/53961>> accessed December 14, 2020
- <https://www.facebook.com/SeyiAwojulugbe>, “NBC to Media Houses: Be Careful How You Report #EndSARS Crisis... Don't Embarrass Govt” (TheCable, October 20, 2020)
<<https://www.thecable.ng/nbc-houses-careful-report-endsars-crisis-dont-embarrass-govt>> accessed December 14, 2020
- Clause 6 (10) of DRFB
- Clause 6 (11) of DRFB. There could be potential conflict with the provision of Section 24 of the Cybercrimes Act.
- Clause 6 (20) of DRFB
- Section 2(b) of the Internet Code of Practice
- Section 3.3 of the Internet Code of Practice
- Section 3.4 of the Internet Code of Practice
- Section 5.3 of the Internet Code of Practice
- Clause 12 (3) of Protection from Internet Falsehood and Manipulation Bill 2019
- Clause 18 and 23 (3) of Protection from Internet Falsehood and Manipulation Bill 2019
- Clause 6 (21) of DRFB
- Section 373 of the Criminal Code Act
- Clause 6 (14) of the DRFB
- Section 24 of the Cybercrimes Act defines and criminalises hate speech
- Article 3.1.1. of NBC Code
- Clause 6 (15) of DRFB
- Clause 6 (16) of DRFB
- 'Analysing The Proposed Hate Speech - Charles Omole' (Analysing The Proposed Hate Speech - Charles Omole) <<https://www.proshareng.com/news/Tech-Regulations---Govt/Analysing-The-Proposed-Hate-Speech---Charles-Omole/48170>> accessed 14 December 2020
- Clause 6 (13) of DRFB
- Clause 4(2) Hate Speech (Prohibition) Bill (HB. 246), 2019

- Hate Speech (Prohibition) Bill (HB. 246), 2019
- Clause 4 of the Hate Speech (Prohibition) Bill (HB. 246), 2019
- Clause 13 (3) of DRFB
- The Incorporated Trustees of Laws and Rights awareness initiatives v Federal Republic of Nigeria. SUIT No ECW/CCJ/APP/53/2018 - JUDGEMENT ECW/CCJ/JUD/16/20 (July 2020) <http://prod.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_16_20.pdf> accessed 14 December 2020
- Clause 6(5) DRFB
- Clause 6(12) DRFB
- Clause 6(12)(d) DRFB
- Clause 6(12)(j) DRFB
- Clause 54 Draft Copyright Bill
- Clause 22 Draft Copyright Bill
- Clauses 9(10) and (11) Draft Copyright Bill
- Clause 6(12)(j) DRFB
- Clause 7 (1) of DRFB
- Clause 7 (5) of DRFB
- Clause 7 (11) of DRFB
- Section 5.3 of Internet Code of Practice mandates the blocking of access to platforms hosting child pornography.
- Section 23 of Cybercrimes Act.
- Section 24 of Cybercrimes Act
- Clause 11(7) DRFB
- "EIU Inclusive Internet Index" (EIU Inclusive Internet Index, 2020) <<https://theinclusiveinternet.eiu.com/explore/countries/NG/performance/indicators/overall>> accessed December 14, 2020
- <https://www.facebook.com/thenicheng>, "Nigeria Crashes Internet Data Prices by Half | TheNiche" (TheNiche, December 10, 2020) <<https://www.thenicheng.com/nigeria-crashes-internet-data-prices-by-half/>> accessed December 14, 2020
- National Broadband Plan 2020-2025
- Muhammed Akinyemi, "The Future of Nigeria's National Broadband Plan 2020-2025 - Space in Africa" (Space in Africa, November 10, 2020) <<https://africanews.space/the-future-of-nigerias-national-broadband-plan-2020-2025/>> accessed December 14, 2020
- "Pantami Receives NBP 2020-2025 Committee Report" (Ncc.gov.ng, February 18, 2020) <<https://www.ncc.gov.ng/media-centre/news-headlines/788-pantami->

receives-nbp-2020-2025-c-ttee-report> accessed December 14, 2020 “

- The Nigerian National Broadband plan, 2020 to 2025, page 38
- When charging, the process should be transparent and reasonable. Clause 7 (1) of DRFB
- In recent time, the government has launched or joined the Open Budget Policy, Open Government Partnership, Open Data Portal and The Nigeria Data Portal.
- “OGP - Budget Office of the Federation - Federal Republic of Nigeria” (Budgetoffice.gov.ng, 2020) <<https://www.budgetoffice.gov.ng/index.php/resources/internal-resources/policy-documents/ogp>> accessed December 14, 2020;
- “Nigeria - Open Government Partnership” (Open Government Partnership, October 26, 2020) <<https://www.opengovpartnership.org/members/nigeria/>> accessed December 14, 2020;
- “Open Data Portal- About OpenData” (Data.gov.ng, 2011) <<http://www.data.gov.ng/about>> accessed December 14, 2020; and
- “Nigeria Data Portal” (Knoema, 2020) <<https://nigeria.opendataforafrica.org/>> accessed December 14, 2020
- Section 15 of Freedom of Information Act and Section 187-196 of the Evidence Act
- The preamble of the FOI Act lists its purpose to include making public records more freely available and to provide for public access to public records and information.
- Article 7 (4) of DRFB
- Military's shutdown of NE Nigeria telecoms disrupts trade, “Military's Shutdown of NE Nigeria Telecoms Disrupts Trade” (The New Humanitarian, June 10, 2013) <<https://www.thenewhumanitarian.org/news/2013/06/11/military-s-shutdown-ne-nigeria-telecoms-disrupts-trade>> accessed December 14, 2020
- Reports reveal that this was heightened during the #EndSars protest where there was a crippling fear that the Internet could be shut down. Yomi Kazeem and Yinka Adegoke, “Nigeria EndSARS Protests Fear Internet Shutdown as Power Cuts Hit” (Quartz Africa, October 21, 2020) <<https://qz.com/africa/1920854/nigeria-endsars-protests-fear-internet-shutdown-as-power-cuts-hit/>> accessed December 14, 2020
- Clause 7 (6) & (7) of DRFB
- Clause 7 (9) of DRFB
- ParadigmHQ, “President Buhari's Secret War on Free Speech - Paradigm Initiative” (Paradigm Initiative, November 17, 2017) <<https://paradigmhq.org/president-buharis-secret-war-on-free-speech/>> accessed December 14, 2020
- Shayera Dark, “#EndSARS: How Nigerians Harness Social Media against Police Abuse” (Aljazeera.com, October 25, 2020)

- <<https://www.aljazeera.com/news/2020/10/25/endsars-how-nigerians-use-social-media-against-police-brutality>> accessed December 14, 2020
- Agency Report, “Lai Mohammed: We Need to 'Dominate', Control What Nigerians Post on Social Media” (Premium Times Nigeria, October 28, 2020)
<<https://www.premiumtimesng.com/news/headlines/423463-lai-mohammed-we-need-to-dominate-control-what-nigerians-post-on-social-media.html>> accessed December 14, 2020
 - “NSA: Protesters Used Social Media to Spread Subversive Contents” (THISDAYLIVE, October 29, 2020) <<https://www.thisdaylive.com/index.php/2020/10/29/nsa-protesters-used-social-media-to-spread-subversive-contents/>> accessed December 14, 2020
 - Senior Editor, “Lagos Lawmaker Says Hoodlums Hijacked #EndSARS Protests Because Protesters Gave Them Food” (NewsWireNGR, October 29, 2020)
<<https://newswirengr.com/2020/10/29/lagos-lawmaker-says-hoodlums-hijacked-endsars-protests-because-protesters-gave-them-food/>> accessed December 14, 2020
 - Clause 12 (3) of Protection from Internet Falsehood and Manipulation Bill 2019
 - Clause 8 (1) DRFB
 - Clause 8 (2) DRFB
 - Section 2 of the Terrorism (Prevention) Act, 2011 and 4 as amended by Section 3 of the Terrorism (Prevention) (Amendment) Act, 2013.
 - Clause 8 (4) of the DRFB
 - Okojie Y and Bolu I, “Competition/Consumer Protection Law A REVIEW OF THE FEDERAL COMPETITION AND CONSUMER PROTECTION BILL, 2016” (2018)
<<http://www.spaajibade.com/resources/wp-content/uploads/2018/06/A-REVIEW-OF-THE-FEDERAL-COMPETITION-AND-CONSUMER-PROTECTION-BILL-2016-Okojie-Bolu.pdf>> accessed December 14, 2020
 - Section 86 (3) of the Federal Competition and Consumer Protection Act (FCCPA)
 - Section 105 (2) of FCCPA
 - Clause 8(5) DRFB
 - Alison Gillwald, Chenai Chair, et al, (September 2016) “Much Ado About Nothing? Zero-rating in The African Context”. Page 3
https://www.researchictafrica.net/publications/Other_publications/2016_RIA_Zero-Rating_Policy_Paper_-_Much_ado_about_nothing.pdf accessed on 14th December, 2020
 - ibid
 - Paragraph 3.1-3.6 of the Draft Code for the Establishment of Internet Industry Code of

Practice in Support of Net Neutrality

- Paragraph 3.6 of the Draft Code for the Establishment of Internet Industry Code of Practice in Support of Net Neutrality
- “The Rules of Fair Play – ‘Net Neutrality in the Nigerian Telecommunications Industry’” (2018) <<https://www.advocaat-law.com/assets/resources/f28a937d499f2d8390d2cc8136c67517.pdf>> accessed on 14th December, 2020
- Section 3.6 of the Internet Code of Practice
- Clause 8(7) DRFB
- HIV AIDS Anti-Discrimination Act 2014
<https://www.ela.law/Templates/media/files/Newsletter_Articles_Clients/MEA/November/The_HIV_and_AIDS_Act_2014.pdf> accessed on 14th December, 2020
- Section 1, Discrimination against Persons with Disabilities (prohibition) Act 2018
- Section 4, HIV and AIDS (Anti-Discrimination) Act 2014
- Section 3.6 of Internet Code of Practice
- Clause 9 (12) of DRFB
- Clause 9 (5) of DRFB
- Clause 9 (9) of DRFB
- Clause 9 (4) of DRFB
- Information disorder manifests in the form of disinformation, misinformation and mal-information. Clause 9 (7) of DRFB
- In Nigeria, an indigenous language is a mandatory requirement for pupils at secondary school, which for a significant part, are confined to the three widely spoken languages in the country. This could lead to erasure of minority ethnic groups and their language.
- Sector 10 (1) of DRFB
- Student Privacy, “Student Privacy” (Electronic Frontier Foundation, 2020)
<<https://www.eff.org/issues/student-privacy>> accessed December 14, 2020
- Chin M, “Exam Anxiety: How Remote Test-Proctoring Is Creeping Students Out” (The Verge, April 29, 2020) <<https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education>> accessed December 14, 2020
- “Understanding the Student Privacy Problem – The Missing Report” (The Missing Report, October 10, 2019) <<https://preyproject.com/blog/en/understanding-the-student-privacy-problem/>> accessed December 14, 2020
- Duball J, “Shift to Online Learning Ignites Student Privacy Concerns” (IAPP.org, April 28, 2020) <<https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/>> accessed December 14, 2020

- Chris Ikosa, "Can Data Protection be Breached in Schools?", <https://www.businessamlive.com/can-data-protection-be-breached-in-schools/#:~:text=An%20unauthorised%20person%20accessing%20data,data%20breaches%20in%20Nigerian%20schools.&text=Schools%20must%20have%20a%20proper,they%20must%20pseudonymise%20the%20data.> , accessed on 25th October, 2020
- African Academic Network on Internet Policy, "PRIVACY AND DATA PROTECTION IN THE NIGERIAN EDUCATIONAL SECTOR" (African Academic Network on Internet Policy - AANoIP, November 22, 2020) <<https://aanoip.org/privacy-and-data-protection-in-the-nigerian-educational-sector/>> accessed December 14, 2020
- Emmanuel Paul, "Hackers Have Access to Data from Nigerian and Kenyan Universities", <https://techpoint.africa/2020/06/01/nigerian-kenyan-universities-hacked/>, accessed on 25th October, 2020.
- Clause 10 (2) of DRFB
- Clause 10 (3) of DRFB
- Clause 10 (8) of DRFB
- Section 2 (1) Copyright Act
- Section 3 (1) (a), (b) Copyright Act
- Section 9, Copyright Act
- Article 2.5 of NDPR
- Article 5.5 of DPIF
- Clause 11, DRFB
- Clause 11 (1), DFRB
- Clause 11 (2), DFRB
- Clause 11 (3), DFRB
- Clause 11(6), (7), DFRB
- 'Nigeria Internet Penetration 2025' (Statista) <<https://www.statista.com/statistics/484918/internet-user-reach-nigeria/>> accessed 14 December 2020
- The failure to adopt e-ticketing at the Kaduna-Abuja train station has promoted corruption and lack of efficiency. "Corruption Galore at Abuja-Kaduna Train Stations | The Guardian Nigeria News - Nigeria and World News" (The Guardian Nigeria News - Nigeria and World News, December 3, 2020) <<https://guardian.ng/opinion/corruption-galore-at-abuja-kaduna-train-stations/>> accessed December 14, 2020
- Clause 12 (3) of DRFB
- "Nigeria - Digital Identification for Development Project" (World Bank, 2020) <<https://www.worldbank.org/en/news/loans-credits/2020/02/18/nigeria-digital->

identification-for-development-project> accessed December 14, 2020

- “Anonymous Claims Hacking of Government’s Websites for #EndSARS” (The Guardian Nigeria News – Nigeria and World News, October 14, 2020) <<https://guardian.ng/news/anonymous-claims-hacking-of-nigerian-governments-websites-in-support-of-endsars/>> accessed December 14, 2020
- An HIV Survey conducted by a government agency was available for sale on the dark web. Simbiat Sadiq, “Protecting Health Information in Nigeria: Lessons From Nigeria HIV/AIDS Indicator And Impact Survey (NAIIS) Data Breach” (CybersecFill, November 10, 2019) <<https://www.cybersecfill.com/protect-health-information-of-nigerian-citizens-a-case-of-nigeria-hiv-aids-indicator-and-impact-survey-data-breach/>> accessed December 14, 2020
- Confidentiality and integrity are principles of data protection that creates the obligation to ensure technical and organisational security measures.
- Privacy notice is a transparency statement to the world about processing of personal data. It is not a policy or a contract. A privacy policy on the other hand is an internal facing document of an organisation about how it handles privacy.
- Clause 2 of DRFB
- Clause 3 (4) of DRFB
- Clause 8 of DRFB
- Clause 8 (4) of DRFB
- Clause 8 (4) of DRFB
- Clause 12 (3) of DRFB
- Section 45(2) of the Cybercrimes Act 2015
- Section 9 of the Lawful Interception of Communication Regulation.
- “Why Encryption Back Doors Threaten Human Rights” (Human Rights Watch, July 8, 2015) <<https://www.hrw.org/news/2015/07/08/why-encryption-back-doors-threaten-human-rights>> accessed December 14, 2020



This work was Commissioned by



with support from



This report is an independent and objective analysis of the digital rights and freedom bill commissioned by Paradigm Initiative with support from Henrich Bill Foundation as part of Paradigm Initiative's advocacy efforts towards the passage of Digital Rights and Freedom Bill into Law in Nigeria.

The report is a useful critic of the bill to help the understanding of its provisions and to look at area of convergence and divergence with existing and proposed laws, addressing subjects similar to the objectives of the bill.

Visit

www.paradigmhq.org

to learn more about PIN's work



paradigmhq

For enquires, send an email to mail@paradigmhq.org.