State of Internet Freedom in Nigeria 2019

Mapping Trends in Government Internet Controls, 1999-2019

January 2020

CIPESA

Table of Contents

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Nigeria, tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Bostwana, Burundi, Cameroon, the DRC, Ethiopia, Kenya, Malawi, Rwanda, Senegal, Tanzania, Uganda, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

CIPESA recognises Adaora Okoli as the main content contributor to this report.

The research was conducted with support from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Federal Ministry for Economic Cooperation and Development (BMZ).

Editors
Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

State of Internet Freedom in Nigeria 2019
Published by CIPESA,
www.cipesa.org
January 2020

1 Introduction

1.1 Introduction

Over the last 20 years, Nigeria, like many African countries, has continued to introduce aggressive and sophisticated measures that potentially curtail internet freedom. These control measures, include the enactment of repressive laws that legalise surveillance and interception of communication, the arrests and intimidation of bloggers and social media users, taxation of online access and criminalisation of online speech and dissent.

For example, Section 29 of the 2011 Terrorism (Prevention) Act allows law enforcement agencies to apply to a judge for an "interception of communication order" for the purpose of preventing a terrorist act or prosecuting offenders under the Act. Meanwhile, section 39 of the Cybercrimes Act allows a judge to order a communication service provider to intercept, collect, record, permit, or assist authorities in collecting or recording content or traffic data associated with specific communications, or authorise a law enforcement officer to collect or record the same.

The government has also introduced e-government and digital identity programmes that require citizens to provide detailed personal information, including biometric data collection for voters' cards, drivers' licences and other services. This has been in addition to the requirements for SIM card registration for all phone subscribers. These measures, though justified by the state, have enhanced the government's surveillance capacity, particularly since there is no transparency or strict judicial oversight over the surveillance activity.

Although ensuring the safety and security of online communication is critical to the enjoyment of digital rights, the implementation of the foregoing measures in the absence of key safeguards, such as a data protection law, is in itself a threat to the very rights sought to be protected. It is therefore important to situate the on-going discussions around internet rights by providing an in-depth analysis of the trends of how government policies and practices have shaped and restricted digital rights in Nigeria over the last 20 years.

1.2 Aim of the Study

This research seeks to document how government controls have affected internet freedom in Nigeria since the year 2000. Specifically, the research focuses on a select set of issues, including the proliferation of retrogressive policies and laws; surveillance and surveillance capacity of the government; digitisation programmes; censorship; and the so-called "new frontiers" such as the introduction of internet related taxes.

The study also sought to identify measures that can secure internet freedom in Nigeria and inform policy makers, the media, academia, technologists, civil society and other researchers on the policy, legal, institutional and practice landscape with a view of identifying opportunities for improvement of the digital space.

2 Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. The literature review included various policy documents, academic works, government documents, and media reports.

Further, the study involved a review of existing and proposed legislation, regulations, directives, case law and procedures that provided an understanding of the trend of government internet controls over the last two decades. Key Informant Interviews (KIIs) were conducted with purposively selected respondents. These included civil society organisations, social media users, telecoms regulators, media houses, human rights defenders and activists, academics, lawyers, staff of telecoms firms, Internet Service Providers, government ministries such as those responsible for ICT and security, as well as semi-autonomous bodies (such as electoral commissions, data protection agencies, and human rights commissions).

3 Country Context

3.1 ICT Status

Like most other African countries, Nigeria had very limited connectivity to the internet by the turn of the 21st century, standing at 78,740 users representing 0.1% of the population.[1] Internet penetration rates have since grown significantly, with the number of internet users reaching 38,261,938 or 24% in 2010; and over 113 million in 2019.[2] As of December 2019, Nigeria had an estimated 184.4 million mobile phone subscribers.[3] Nigeria has a vibrant and growing internet user population, enabled by a strong and innovative technology sector. The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed internet service providers (ISPs) rising from 18 in 2000 to 82 as of May 2017.[4]

In 2003, the government enacted the Nigeria Communications Act that provided for a regulatory framework for the communications industry in the country, including the establishment of the Nigeria Communications Commission (NCC) as well as the Universal Access Fund.[5] The Act also repealed the 1992 Nigeria Communications Commission Act. It has been reported that although the government nominates the NCC's nine-member board of commissioners, the regulator's decisions have been viewed as relatively independent.[6]

In 2007, the government enacted the National Information Technology Development Agency (NITDA) Act[7] that established the National Information Technology Development Agency (NITDA) with the mandate to "create a framework for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria."[8]

1 *Nigeria Internet Users; https://www.internetlivestats.com/internet-users/nigeria/*
2 *https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-5*
3 *https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#gsm*
4 *Freedom House (2017) Freedom on the Net/Nigeria https://freedomhouse.org/report/freedom-net/2017/nigeria*
5 *Nigeria Communications Act 2003; https://www.ncc.gov.ng/accessible/documents/128-nigerian-communications-act-2003/file*
6 *Freedom House (2017) Freedom on the Net/Nigeria https://freedomhouse.org/report/freedom-net/2017/nigeria*
7 *National Information Technology Development Agency Act https://nitda.gov.ng/wp-content/uploads/2019/03/NITDA-ACT-2007-2019-Edition.pdf*
8 *Section 6(a) of the NITDA Act*

3.2 Political Environment

Prior to 1999, politics in Nigeria was marked by coups and mostly military rule, until the death in 1998 of the then military head of state, Gen. Sani Abacha,[9] allowed for a political transition. In 1999, a new constitution was adopted and a peaceful transition to civilian government was completed, after the election of President Olusegun Obasanjo.[10] However, the government continues to face the daunting task of institutionalising democracy and reforming a petroleum-based economy, whose revenues have been squandered through decades of corruption and mismanagement.[11] Although both the 2003 and 2007 presidential elections were marred by significant irregularities and violence, Nigeria is currently experiencing its longest period of civilian rule since independence.

According to the 2018 Democracy Index report, Nigeria is considered a hybrid regime of democracy, putting it in the same category as countries like Kenya, Sierra Leone, Gambia and Cote D'Ivoire.[12] While elections have been held consistently every four years since 1999, they have had substantial irregularities preventing them from being free and fair. The 2015 election was also heralded since the then-umbrella opposition party, the All Progressives Congress, defeated the long-ruling People's Democratic Party that had governed the country since 1999, and assumed the presidency, marking the first peaceful transfer of power from one party to another. Presidential and legislative elections held in early 2019 were deemed broadly free and fair despite voting irregularities, intimidation, and violence.[13]

3.3. Economic Status

Like many other African countries, Nigeria's economy was also struggling as of 1999. The country's GDP growth rate for 1999 stood at 0.47% and peaked in 2004 at 33.7%. Between 2004 and 2013, the growth rate was reported to be 6%.[14]

Although the country relies heavily on oil as its main source of foreign exchange earnings and government revenues, following the 2008-09 global financial crises, the banking sector was effectively recapitalised, and regulation enhanced.[15] Since then, Nigeria's economic growth has been driven by growth in agriculture, telecommunications, and services. However, the economic diversification and strong growth have not translated into a significant decline in poverty levels, as over 62% of Nigeria's over 180 million people still live in extreme poverty.[16] Figures from the International Monetary Fund IMF) show that as of 2019, Nigeria's GDP per capita (PPP) was USD 6,027.[17]

Despite its strong fundamentals, the development of the oil-rich nation has been hampered by inadequate power supply, lack of infrastructure, delays in the passage of legislative reforms, an inefficient property registration system, restrictive trade policies, an inconsistent regulatory environment, a slow and ineffective judicial system, unreliable dispute resolution mechanisms, insecurity, and pervasive corruption.[18]

9 *Gen. Sani Abacha, https://www.bbc.co.uk/news/resources/idt-f9f1cd17-2c50-442e-88fc-e2deb46dbde1*
10 *Nigeria. Presidential Elections 1999; https://www.electoralgeography.com/new/en/countries/n/nigeria/nigeria-presidential-election-1999.html*
11 *Africa: Nigeria; https://www.cia.gov/library/publications/the-world-factbook/geos/print_ni.html*
12 *Democracy Index 2018: https://qz.com/africa/894326/nigeria-south-africa-kenya-and-tanzania-fail-to-improve-on-global-corruption-index/*
13 *Africa: Nigeria; https://www.cia.gov/library/publications/the-world-factbook/geos/print_ni.html*
14 *Nigeria's GDP falls to lowest since 1999; https://www.thecable.ng/nigerias-gdp-growth-falls-to-lowest-since-1999*
15 *Africa: Nigeria; https://www.cia.gov/library/publications/the-world-factbook/geos/print_ni.html*
16 *Ibid*
17 *World Economic Outlook Database, April 2019 http://tiny.cc/3308bz*
18 *Africa: Nigeria; https://www.cia.gov/library/publications/the-world-factbook/geos/print_ni.html*

4 Results

4.1 Key Trends of the Internet Control Over the Last Two Decades

4.1.1 Weaponising the Law to Legitimise Actions

Nigeria has had a history of repressive laws from its pre-1999 military era and others from the fledgling democracy era from 2000. Although the 1999 Constitution of the Federal Republic of Nigeria (as amended) under chapter 4 provides for the rights to a fair hearing, privacy and freedom of expression, respectively,[19] a number of laws and policies were enacted over the study period that negatively affect internet rights in the country. Older laws in existence also undermine free expression and government openness. For example, Section 1 of the Official Secrets Act criminalises the sharing of classified matters without authorisation.[20] As a result, civil servants have for decades been afraid to release information, a chokehold that continues to-date.[21]

In addition, the Criminal Code makes it a penal offence for any civil servant to give out official information. Section 97(1) of the law provides that: "Any person who being employed in the public service, publishes or communicates any fact which comes to his knowledge by virtue of his office and which it is his duty to keep secret, or any document which comes to this possession by virtue of this office and which it is his duty to keep secret, except to some person to whom he is bound to public or communicate it, is guilty of a misdemeanor, and is liable to imprisonment for two years."

19 *Sections 36, 37 and 39 of the Nigeria Constitution,*

20 *S1 of the Official Secrets Act, provides amongst other things, that: "...a person who - (a) transmits any classified matter to a person to whom he is not authorised on behalf of the government transmit it, or (b) obtains, reproduces or retains any classified matter which he is not authorised on behalf of the government to obtain, reproduce or retain, as the case may be, shall be guilty of an offence." Any person who commits an offence under this provision is liable on conviction, or indictment, to imprisonment for a term not exceeding 14 years, and on summary conviction, to imprisonment for a term not exceeding two years or a fine of an amount not exceeding N200 or to both such imprisonment and fine.*

21 *Unlocking Nigeria's closet of secrecy- a report on the campaign for a freedom of information Act in Nigeria; https://tinyurl.com/uenswkr; Campaigning for Access to Information in Nigeria A Report of the Legislative Advocacy Programme for the Enactment of a Freedom of Information Act;https://tinyurl.com/w4gov5u*

Legalising Surveillance and Interception of Communication

Like in other African countries, the fight against terrorism has been used as a basis for introducing repressive laws that legitimise surveillance and the interception of communication in Nigeria. Section 29 of the 2011 Terrorism (Prevention) Act allows law enforcement agencies — with the approval of the Attorney General and the Coordinator on National Security — to apply to a judge for an "interception of communication order" for the purpose of preventing a terrorist act or prosecuting offenders under the Act. Communication service providers can be required to intercept and retain specified communications, or the law enforcement actors may enter any premises to install any device for the interception and retention of communications.

2015 Cybercrimes (Prohibition, Prevention, etc) Act sets out a separate regime for communications surveillance. Under Section 39, a judge may order a communication service provider to intercept, collect, record, permit, or assist authorities in collecting or recording content or traffic data associated with specific communications, or authorise a law enforcement officer to collect or record the same, where there are "reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings."

Additionally, under the 2013 Nigeria Communications Commission (NCC) Guidelines for the Provision of Internet Service, ISPs are required to comply with and provide any service related information requested by the Commission or other legal authority, including information regarding particular users and the content of their communications, subject to any other applicable laws of Nigeria.[22]

Silencing Dissent and Criticism through Criminalising Free Speech

The systematic use of criminal law to prosecute and punish critics has become a trend in Nigeria. Different provisions in laws have been enacted and used to tackle "fake news". In May 2015, Nigeria introduced the Cyber Crime (Prohibition, Prevention etc) Act meant to provide a framework for the prohibition, prevention, prosecution and investigation of cybercrimes. Section 24 of the law penalises "cyberstalking" and online publication of messages a person "knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another." This provision has been used to arrest several bloggers and online journalists on charges of "cyberstalking" stemming mostly from articles critical of the government.[23]

Between 2016 and 2017, at least eight social media users, activists, and journalists were arrested under the Cybercrime Act for their online posts.[24] In July 2017, journalist Danjuma Katsina was arrested in Katsina state following Facebook comments on corruption allegations against Mansur Mashi, a newly elected member of the House of Representatives. He was released after one day and given no reason for his detention.[25] In July 2017, a primary school teacher was fired and then arraigned before a Magistrate's court in Ilorin for allegedly insulting Senate President Bukola Saraki on Facebook. However, the charges were later withdrawn.[26] In February 2018, Nigeria's secret police arrested journalist Tony Ezimakor over his reporting that alleged that the government secretly paid millions of dollars to secure the release of the girls kidnapped by the Boko Haram militants in Chibok in 2014.[27]

22 Section 6(c) of the Guidelines, https://tinyurl.com/s87q5s8

23 How Nigeria's cybercrime law is being used to try to muzzle the press, https://tinyurl.com/yc2zp27l

24 Freedom of the Net Nigeria https://freedomhouse.org/report/freedom-net/2018/nigeria

25 Abdulaziz Abdulaziz, Police detain Nigerian journalist over Facebook post, http://bit.ly/2fLY6lu

26 Nnenna Ibeh, UPDATED: Charges against Kwara civil servant who criticized Saraki withdrawn, Naij.com, http://bit.ly/2xwvT9E

27 Daily Independent's Bureau Chief Still in DSS Detention, https://tinyurl.com/vgeslxx

In August 2019, Omoyele Sowore, a publisher of Sahara Reporters, and an opposition presidential candidates during the February 2019 presidential election, was arrested for treasonable felony for using his social media and online platforms to call for protests in August 2019 against bad governance under the #RevolutionNow movement.[28]

In December 2015, the government attempted to pass the controversial Frivolous Petitions Prohibition Bill which was later withdrawn in May 2016, following protests by citizens and advocacy by civil society organisations. In March 2018, Nigeria introduced the widely controversial Hate Speech Bill before the Senate to tackle hate speech and defamation online. The move raised concerns of the possibility of its use to stifle freedom of expression and silence government critics.

Shortly thereafter, in June 2018, the Nigerian Senate announced the introduction of a new bill to regulate social media use.[29] The announcement came months after the Senate had passed the Digital Rights and Freedom Bill first proposed in April 2015. In March 2019, Nigeria's President Buhari declined to assent to the Bill. This Bill had been approved by the House of Representatives in December 2017 and the Senate in March 2018.[30] The Bill had sought to provide for the protection of human rights online, 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 and digital media and for related matters. In a letter to the Senate, the president stated that the bill covered too many technical subjects and failed to address any of them extensively. It remains to be seen whether the Senate will address the President's concerns and return the Bill for assent.

4.1.2 Disrupting Networks – From SMS Censorship to Social Media Blockage

The use of network disruptions in Nigeria is a recent phenomena with the first incident reported in the summer of 2013, when the Nigerian military, as part of its counter insurgency operations against Boko Haram insurgents, reportedly shut down GSM mobile telephony in three northeast states – Adamawa, Borno and Yobe.[31] Although the mobile phone shutdown was 'successful' from a military-tactical point of view, it angered citizens and engendered negative opinions toward the state and new emergency policies. The reported "success" seemed to have emboldened the government such that in November 2017, the NCC and the national security adviser ordered internet service providers to block 21 websites. Following tests done by Paradigm Initiative and the Open Observatory of Network Interference (OONI), it was discovered that the blocked sites largely promoted the independence of Biafra, the region that attempted to secede from Nigeria in 1967 in the Biafran War. The common techniques adopted by ISPs included TCP/IP blocking by Globacom, DNS tampering by MTN and blocking the HTTP layer by Airtel.[32]

28 DSS arrests AAC presidential candidate, Omoyele Sowore, https://tinyurl.com/qvnjdp5

29 Nigeria and the Obsession to Regulate Social Media, https://tinyurl.com/r3d6vbj

30 Nigeria's president refused to sign its digital rights bill, what happens now? https://tinyurl.com/sk2g9ap

31 Silencing Boko Haram: Mobile Phone Blackout and Counterinsurgency in Nigeria's Northeast region, https://www.stabilityjournal.org/articles/10.5334/sta.ey/

32 Measuring Internet Censorship in Nigeria, https://tinyurl.com/raofpct

4.1.3 The Push Towards Determining Identity Amidst Poor Oversight

The ability and desire to digitally identify any telecommunication services user with precision has become an obsession for most governments on the continent, including Nigeria. The government has thus continuously introduced measures, including enacting of laws that would legitimise the surveillance and interception of communication, mandatory SIM card registration as well as adoption of biometric data collection programs.

Mandatory SIM Card Registration

In November 2011, the Nigeria Communications Commission issued the Communications Commission (Registration of Telephone Subscribers) Regulations (2011), which require mobile phone subscribers to allow their fingerprints and a biometric map of their faces to be collected and registered to their SIM card, which are then stored in a central government database.[33]

Prior to the issuance of regulations, the Communications Commission, in collaboration with the National Identity Management Commission (NIMC) had issued a request for proposals[34] from private sector software companies to provide services in the conceptualisation, setup and operations of the SIM Card Identity Management System and to create and integrate the registration process into the Mobile Operators existing structure of sales and service delivery. The goals of the SIM card management are to integrate various existing operator subscriber records in the country, expand the scope of records requirement from subscribers, and build a comprehensive database of all pre-paid and post-paid mobile phone subscribers for further linkage into the National Identity Card system to create a centralised database of all SIM card subscribers in Nigeria.

In 2013, the communications regulator was reported to have issued a directive to all cyber cafe owners and operators to register and maintain a database of users of their services. Cyber café operators were to register users' full names, physical addresses, telephone numbers, and to take their passport photos and telephone numbers.[35] According to the notice, the NCC claimed to have noticed the increasing rate of cyber crime in the country. Moreover, that most of it was reportedly committed through use of cyber cafes, making it harder for the regulator to carry out investigations.[36]

33 NCC Registration of Telephone Subscribers Regulations 2011, https://tinyurl.com/wwjoh99

34 NCC Request for Proposals; https://www.nimc.gov.ng//docs/adverts/NCC_SIM_Registration_RFP.pdf

35 Cyber Cafes in Nigeria Asked to Register Users to Help Fight Cyber Crime, https://tinyurl.com/vsuo6da

36 Ibid

Rapid Adoption of Biometric Data Collection

In 2014, the government formally launched a national electronic identity card, 10 years after the first attempt failed. The new cards show a person's photograph, name, age and unique ID number. Further, 10 fingerprints and an iris are scanned during enrolment.[37] The NIMC, which is behind the rollout, is trying to integrate several government databases including those for driving licences, voter registration, health insurance, taxes and pensions.[38] Registered citizens, are citizens of Nigeria as well as other legal residents in the country, were also to be assigned unique National Identification Number (NIN) and issued with General Multi-Purpose Cards (GMPC).[39]

In September 2018, Nigeria's Federal Executive Council (FEC) approved the immediate commencement of the implementation of a strategic roadmap for Digital Identity Ecosystem in Nigeria.[40] According to the NIMC, the process will see the effective and efficient mass enrolment of citizens and legal residents into a centralised, secure National Identity Database. Digital identities in the form of the National Identification Number (NIN) will be issued, and their use made mandatory for transactions from January 2019.[41] The NIN is now a compulsory requirement to obtain the Nigerian International Passport, and it is mandatory for all workers under the Contributory Pension Scheme to produce their NIN as part of their pension requirements.[42] Only about 39 million people had fully registered for their NINs by October 2019.[43] Notably, there has been poor oversight and supervision of this data gathering. Whats of concern is that Nigeria currently does not have a data protection law but only data protection guidelines issued by NITDA.[44]

Various government agencies in Nigeria collect citizens' data through their individual biometric data collection programmes. The agencies include the Central Bank of Nigeria, the Federal Road Safety Commission, the Federal Inland Revenue Service, the National Pension Commission, the Independent National Electoral Commission, the National Health Insurance Scheme, the National Population Commission, Telecom Service Providers and the Federal Ministry of Agriculture and Rural Development. This effectively leads to a duplicity of efforts and storage of the same biometric data by multiple agencies and weakness in data security especially in the absence of a comprehensive data protection law to protect this data. Thus, there has been a push by both civil society and some legislators for the harmonisation of data collection and co-ordinated oversight in order to address privacy concerns.[45]

37 BBC (2014) Nigeria launches national electronic ID Cards; https://www.bbc.com/news/world-africa-28970411

38 Ibid

39 National Identity Card: Another bumpy road to building national database, https://tinyurl.com/uy6993k

40 FEC Approves Implementation of Strategic Roadmap for Digital Identity Ecosystem in Nigeria, https://tinyurl.com/t2bskxk

41 The Digital Identity Ecosystem https://www.nimc.gov.ng/digital-identity-ecosystem/

42 National Identity Card: Another bumpy road to building national database, https://tinyurl.com/uy6993k

43 39m Nigerians now have NINs – NIMC, https://tinyurl.com/vnv5ddq

44 See the regulations here: https://tinyurl.com/sl54hdm

45 Reps seek harmonisation of biometric data of Nigerians, https://tinyurl.com/sp4t2g6

4.1.4 The Era of Social Media and Data Taxation

One of the notable and concerning phenomena in recent years is the use of taxation to undermine citizens' use of the internet. In some instances, such measures have been designed partly as a clear measure to limit the number of citizens who can access digital technologies and their use to hold their governments to account.

In March 2016, the Nigerian government introduced the Communication Service Tax Bill which proposed to impose a 9% tax on communication services, such as SMS, data, and voice services. However, civil society groups and social media users carried out online protests against the bill and it was shelved thereafter. Nevertheless, a proposal for a similar tax was made in August 2019 by the Federal Inland Revenue Service seeking to enforce a 5% Value Added Tax (VAT) for online purchases with a bank card, planned to be in place by early 2020.[46] The proposal has not been well received by e-commerce companies.

4.2 Key Positive Developments

Despite the negative trends witnessed in Nigeria, there were notable developments that were indeed positive and support the enjoyment of internet freedom. The two major developments included the robust advocacy and push-back by non-state actors, and the adoption of progressive legislation.

4.2.1 Robust Advocacy and Push-back by Non-State Actors

Non-state actors have continued to be in the forefront of advocacy on internet freedom. Advocacy efforts by civil society in Nigeria led to the development of the Digital Rights and Freedom Bill 2016, which despite obtaining Senate approval was returned to the Senate following President Buhari's decision not to assent to it.

Meanwhile, Nigerian civil society including organisations such as Paradigm Initiative and Media Rights Agenda have filed cases and advocated against the draconian and restrictive legislation adopted by the government, such as the Cybercrime law. They have also formed coalitions, such as the Freedom of Information coalition, and organised training on digital rights including with law enforcement officials on the Cybercrime Act 2015.[47]

46 Nigeria wants to start charging a tax on local online purchases, https://tinyurl.com/rbq7rjp

47 Nigeria: Trends in Freedom of Expression in the Telecommunications and the Internet Sect, https://tinyurl.com/u9zn9xl

4.2.2 Adoption of Progressive Legislation

There are laws in Nigeria that partly protect the freedom of internet users through the recognition of certain civil liberties. An example of such protection is the Advance Fee Fraud Act 2006, which demands that a warrant be obtained before telecommunication data can be obtained by security agencies.[48]

Similarly, the Freedom of Information (FOI) Act 2011[49] is the law that gives effect to citizens the right to access information from government institutions and agencies. Section 1 of the FOI Act provides that: 'Notwithstanding anything contained in any other Act, law or regulation, the right of any person to access or request information, whether or not contained in any written form, which is in the custody or possession of any public official, agency or institution howsoever described, is established". If properly implemented, it will ensure the realisation of the right to freedom of information. The FOI Act was a culmination of civil society efforts led by Media Rights Agenda, Civil Liberties Organisation and the Nigerian Union of Journalists.[50] It took about 18 years between the first draft of the Bill and enactment of the law in May 2011.[51]

However, a major challenge to the implementation of the FOI Act is that it contains some inherent deficiencies. There are a number of sections, such as 11, 12, 14, 15,16, which provide for exemptions to certain types of information requests. These include personal information, information on court proceedings, information considered injurious to the defence of Nigeria, and trade secrets. Exceptions should ordinarily be clearly and narrowly drawn and be restricted to 'harm' and public interest tests.[52]

Although Nigeria does not have a dedicated data protection law, in 2019, the National Information Technology Development Agency (NITDA) issued the Data Protection Regulations 2019. The Regulations apply to transactions intended for or requiring the processing of personal data for all Nigerians who are resident and non-resident, and to non-Nigerians resident in Nigeria.[53]

48 Advance Fee Fraud and other Fraud Related Offences Act, https://tinyurl.com/qtadag6

49 https://www.cbn.gov.ng/FOI/Freedom%20Of%20Information%20Act.pdf

50 Unlocking Nigeria's closet of secrecy: a report on the campaign for a freedom of information Act in Nigeria, August 2000, Media Rights Agenda . http://www.mediarightsagenda.org/pdf%20files/Unlocking%20Nigeria's%20Closet%20of%20Secrecy.pdf

51 The Freedom of Information Act 2011 (FOI) - What It Means For You, https://tinyurl.com/upylk49

52 Obstacles to the Implementation of the Freedom of Information Act, 2011 in Nigeria, https://tinyurl.com/r25g3be

53 Section 1.2(a) of the Data Protection Regulations 2019

5 Conclusion and Recommendations

5.1 Conclusions

The research findings show that while access to and usage of internet has exponentially increased in Nigeria, the country faces a lot of challenges in advancing the benefits that come with the new technologies. Since 1999, successive governments have developed and passed a series of laws and policies that contain retrogressive provisions that legitimise surveillance and the interception of private communication, as well as criminalising dissent and criticism.

The government has also employed other control measures, including the arrests and intimidation of bloggers, journalists and other online community members for their online activities. For example, between 2016 and 2017, at least eight social media users, activists, and journalists were arrested under the Cybercrime Act for their online posts, a scenario that promotes online self-censorship. The government has moved further to introduce digital identification programs, including the mandatory SIM card registration which requires capturing of biometric data of users. All these measures have had a negative effect as they discourage would be online users from engaging in online activities for fear of being victimised. Equally, repeated attempts to introduce laws that will further criminalise the use of social media and other digital technologies, while denying presidential assent to the Digital Rights and Freedom Bill, show that the stance of the Nigerian government is for increased repressive state control over the internet as opposed to greater citizens' internet freedom.

5.2 Recommendations

Government

- Government needs to be more open and attentive to stakeholders in the ICT sector. It should involve more stakeholders before and during the development of laws and policies.
- The Cybercrime Act needs to be amended to expunge section 24 that currently limit internet freedoms .
- The Digital Rights and Freedom Bill should be signed into law before the end of 2020, to further enable protection of the digital rights of citizens.

Private companies

- Adopt and implement the UN Business and Human Rights principles and safeguard the rights of customers by default.
- Private companies' terms and conditions of privacy and data usage must be clear, and should be popularised among users.
- Businesses should support civil society efforts to grow awareness about the need for respect for privacy, data protection and other digital rights.

Media

- Media houses should hold the government to account in ensuring that internet freedoms are protected.
- The media should report stories accurately and responsibly especially in the era of citizen journalism to avoid legal and legislative action on issues such as hate speech, which would stifle the media.
- The media should be more proactive in the reportage and call for adoption of other positive laws and best practices such as those from other regions such as the GDPR.

Civil Society

- Civil society should monitor and serve as an advocacy body and a watchdog on government implementation of laws, regulations and policies. It should therefore continuously watch government actions and decisions and hold it accountable.
- Civil society should not relent in advocacy and lobbying for passage of important bills and policies that will protect internet freedom such as the Digital Rights and Freedom Bill.
- Civil society should engage more robustly and regularly with the government and build better relations with government departments to further advance advocacy on internet freedom matters.

Academia

- The academia the do more original research on internet freedom matters that will bring solutions to addressing the shrinking digital space in Nigeria.
- Academia should include internet freedom in their curriculum to ensure students are made aware of the issues that fundamentally affect digital rights and internet freedoms.
- Collaborate and work with other stakeholders so as to promote internet freedom.

Technical community

- They should educate stakeholders on the impact of new technologies on internet freedom.
- They should develop and promote local platforms to promote public engagement and internet freedom.
- They should develop and promote innovative technologies to circumvent internet control restrictions and surveillance.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org