DOMESTIC REGULATION OF THE CYBERSPACE: AN APPRAISAL OF THE IMPACT OF THE NIGERIAN CYBERCRIME ACT ON THE RIGHTS TO FREEDOM OF EXPRESSION AND PRIVACY GUARANTEED UNDER THE NIGERIAN LAW*

Abstract

The Development of cyber technology has given rise to unprecedented surge in information traffic around the globe. Unfortunately, cybercrimes have equally risen in equal proportion as cyber criminals go on in rampage. The surging rise in cybercrimes has led to the global challenge for a comprehensive and effective laws aimed at addressing the menace of cybercrimes by preventing and punishing cybercrime offenders. Thus by 2015, Nigeria joined the League of Nations that enacted domestic legislation for the prevention and punishment of cyber criminals. This work, using the Nigerian Cybercrimes Act of 2015 as a case study, critically examined the extant provisions of the Act that impacts on the rights of expression and privacy guaranteed by the Nigerian Constitution. The methodology adopted in this work is doctrinaire as we analysed constitutional and legislative instruments. We found some provisions of the Act as violating the constitutional rights to freedom of expression and privacy of Nigerians and recommended modifications.

Keywords: Cyber-regulation, cybercrimes, cyber law, freedom of expression, right to privacy

1. Introduction

The Information Age is a contemporary era in human history identified by the access and control of information and the subsequent transition from industrial production to computerized production.[1] This 'age of information' is associated with the invention of personal computers and, consequently, more advanced developments; such as microprocessors that can process enormous loads of information in very short periods of time and fibre optic internet cables that make it possible to transfer data at a speed of hundreds of megabytes per second.[2] Such technological advancements allowed the general population to have access to the most modern pieces of technologies, such as Smartphones, ipads, tablets, and lap top computers and other electronic processing devices which are now commonly used. The impact of the internet is indeed enormous and revolutionary.[3] As a result of the use of internet, interaction has improved amongst persons with the free exchange of information, ideas, skills and technology. Its influence on the society has been so remarkable that there is hardly anyone who hasn't felt its impact either directly or indirectly. The rapid rise in the use of modern technology around the world has also triggered new challenges. The phenomenon of cybercrime has spread and escalated at a fast rate, alongside the expansion of cyberspace itself as almost over half and a quarter of the world population now own smart phones and have access to the internet. New platforms for different kinds of crimes, human rights abuse and other infringement of personal and corporate rights have been created. These have given rise to a lot of discuss on the need for legislations regulating the Cyber Space.

In Nigeria Cybercrime has become a common phenomenon as more people especially young persons' engage in it on the social media platforms.[4] This is carried out in various ways and a common trend is hacking into people's social media account and using it to defraud people and also posting indecent imagery of persons online such as naked pictures or videos of persons in order to humiliate or blackmail them.[5] Other prevalent forms include; web cloning, phishing, online lottery fraud, job scam, identity theft, credit card fraud, impersonation, romance scam, BVN Scam, spoofing etc. This new crime is denting and drilling holes in the economy of the nation as well. For example, in a recent report by the Internet Crime Complaint Centre which is a partnership between the FBI and America's National White Collar Crime Centre, it was revealed that Nigeria now ranked third among the list of top ten sources of cybercrime in the world.[6] Also the Central Bank of Nigeria (CBN) in its banking sector

***By Emmanuel Ibiam AMAH, PhD,** Senior Lecturer Faculty of Law, Ebonyi State University, Abakaliki, Nigeria**.** Email: amaibiam@gmail.com; and

***Kelechi Markson MBAM,** School of Postgraduate Studies, Ebonyi State University, Abakaliki, Nigeria. Email: kelechimbam@gmail.com

[1] A. Habirovs, 'Factors That Shape Cybercrime Victimization and Use of Prevention Measures in England and Wales.' <http://eprints.hud.ac.uk/id/eprint/35042/> Accessed October 1, 2022.

[2]Ibid

[3]T. Anderson and B. Sturm, 'Cyber bullying: From playground to computer', <https://taraandersongold. files.wordpress.com/2015/11/cyberbullying-from-playground-to-computer.pdf> accessed on 29 August 2022

[4] A. Aderian, 'Cyberbullying in Nigeria: Examining the Adequacy of Legal Responses', *International Journal for the Semiotics of Law*,<https://www.semanticscholar.org/paper/Cyberbullying-in-Nigeria%3A-Examining-the-Adequacy-of-Adediran/59c5653910ff1a457d23c6f5e2b4e2a6bda2b929> accessed 29 August 2022

[5]Ibid

[6]Abdulhamid *and others,* 'Cybercrimes and the Nigeria Academic Institution Networks'. in *the IUP Journal of Information Technology*, 2016 VII (1) 11

supervision report revealed that the Nigeria banking sector lost 7.2 billion naira to internet fraud.[7] The Loss of 7.2 billion naira in a developing economy such as Nigeria' is not something to be proud about.

Apart from the destruction cyber-crime does to the economy, it also leads to the erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women the rewards of e-commerce. France today requires web camera verification for most online business transactions from Nigeria.[8]In Nigeria, cybercrime has been indigenously named 'Yahoo yahoo'[9] while the perpetrators are called 'yahoo boys'.[10] Last year, it was reported that about 782 out of the 978 convictions by the Economic and Financial Crimes Commission (EFCC) were cybercrime related.[11] Apart from the economic loss, cybercrime has created in the eyes of the rest of the world a negative stereotype towards Nigerians. This has tarnished Nigeria's image at the international front. Consequently, Nigerians are treated with suspicion and scepticism in most foreign business dealings. Currently, investor confidence in Nigeria is abysmally poor and it has resulted in low foreign investment and a depressed economy.[12] These and many more justify the dire need for the regulation of the use of the cyber space; hence the national assembly of the federal republic of Nigeria enacted the Nigerian cybercrimes Act of 2015[13] in order to curb the menace of cybercrimes.

The regulation of cyberspace however possesses its own challenges. Among these challenges is the impact of cyber regulation on the human rights of citizens especially the fundamental rights to freedom of expression and privacy. This is basically because the attempt to regulate information that people may post on the internet or information that may be accessible to the public will directly touch on peoples' fundamental rights to express themselves and to be free from state censorship; an integral part of the right to privacy. Authoritarian regimes may also use the internet to propagate their own version of the 'story' unchecked while on the other hand clamping down on differing or opposing information.[14]

This work, using the Nigerian Cybercrimes Act of 2015 as a case study critically examined the extant provisions of the Act[15] and its impacts on the rights of expression and privacy. It reviewed decisions of Nigerian courts and the ECOWAS court on whether the Nigerian Cybercrime Act violates the rights of privacy and freedom of expressions as guaranteed under the Nigerian constitution as well as the African Charter on Human and Peoples rights. It also considered decision of foreign courts on the similar provisions to the Cybercrime Act.

---

[7] A. Ajewole, 'Curbing Cybercrime in Nigeria: Fighting the Masked Enemy and Promoting Productive Alternative for the Youth', <http/www.primopdf.com.> Accessed October 3. 2022.

[8] O.B. Longe and others, 'Cyber Crime and Criminality in Nigeria: what Roles are Internet access points in Playing'<https://www.semanticscholar.org/paper/CYBER-CRIME-AND-CRIMINALITY-IN-NIGERIA%3A-WHAT-ROLES-Longe-Chiemeke/9f3c5f1b69dbe5b6502d34bec8b4022fa03633a6>accessed 3October, 2022.

[9] Nigerian word for cyber fraud, see, T. Akinboyo, 'ANALYSIS: Despite govt clampdown, "yahoo-yahoo" thrives in Nigeria', Premiumtimes, May 3 2021 <https://www.premiumtimesng.com/news/headlines/459089-analysis-despite-govt-clampdown-yahoo-yahoo-thrives-in-nigeria.html> access 17 March 2023; Abbas Muhammad, 'Nigerian youth and ''yahoo yahoo": a Disturbing Trend that must be Halted', *Economic Confidential*, September 30 2022 <https://economicconfidential.com/2022/09/nigerian-youth-yahoo-yahoo/> access 17 March 2023

[10] 'Yahoo boys' are expression used in Nigeria to describe youths involved in cybercrime using electronic e-mails. This social tag originated via the mode employed by yahoo boys in defrauding, which involves sending sinister and deceptive e-mails using hotmail, gmail, yahoo mail and the likes.
'Yahoo boys', <http://naijalingo.com/words/yahoo-boys>access 17 March 2023
Oludayo Tade, 'meet the "yahoo boys"- Nigerian's Undergraduate Conmen, <https://www.usnews.com/news/best-countries/articles/2016-07-28/meet-the-yahoo-boys-nigerias-undergraduate-conmen>access 17 March 2023; Wiktionary, 'yahoo boy' <https://en.m.wiktionary.org/wiki/yahoo_boy>access 17 March 2023

[11]The Guardian, 80% of EFCC's 978 Convictions Cybercrime-related <https:/guardian.ng/news/80-of-efces-978-convictions-cybercrime-related> accessed 16 May, 2/22

[12] S. Ogunlere, 'Impact of Cyber Crimes on Nigerian Economy' International Journal of Engineering and Science 2013) (2) (4) 50.

[13] Cybercrimes (Prohibition, Prevention Etc.) Act, 2015 hereinafter referred to as the' Cybercrime Act' or 'the Act'.

[14]In June 2021, the government of Nigeria suspended Twitter till January 2022 as a retaliation for the action of Twitter in deleting the tweets and account of President Muhammadu Buhari for "contents that threatens or incite violence" the government justified its action on the premise that Twitter had allowed its platform to be used 'for activities that are capable for undermining Nigeria's corporate existence" see <https://twitter.com/FMICNigeria/status/1400843062641717249?ref_asrc=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1400843062641717249%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.nytimes.com%2F2021%2F06%2F05%2Fworld%2Fafrica%2Fnigeria-twitter-president.html> accessed 16 May 2022

[15] Cybercrimes (Prohibition, Prevention, Etc) Act, 2015

2. Cybercrime (Prohibition, Prevention Etc.) Act 2015

The Nigerian Cybercrime Act, 2015 is a novel piece of legislation in that it is the first Nigerian Federal legislation specifically enacted to deal with crimes, commissions, omissions and threats faced in the cyber world in this digital age. The Cybercrime Act 2015 is an Act that provides for the Prohibition, Prevention, Detection and Prosecution of Cybercrime and other related matters in Nigeria. There exist some novel provisions which regulate the use of the cyberspace through the conferment of protection on users and punishment of offenders.

The Act confers protection on the critical National Information Infrastructures.[16] It provides for the designation of certain computer systems, and or networks whether physical or virtual and or the computer programs, computer data and/or traffic data that are vital to Nigeria as constituting Critical National Information Infrastructure.[17] It as well provided punishment for interference with such designated Critical National Infrastructure.[18] The Act in a bid to protect critical National Infrastructure makes it an offence when there is an unauthorized access to a computer for fraudulent purpose and for obtaining data vital to national security.[19] Where such offence is committed with the intent of securing access to classified information relating to commercial or industrial secret, the offence is punishable with imprisonment for a term not more than seven years or a fine of not more than five million naira or 7 years imprisonment or to both fine and imprisonment.[20]

Section 14 of the Act makes it an offence to be engaged in computer related fraud. It provides that any person employed by or under the authority of any bank or other financial institutions and with intent to defraud, directly or indirectly diverts electronic mails shall be guilty of an offence and on conviction, shall be liable to imprisonment. Section 14(4)(b) of the Act makes a very interesting provision which is novel in the Nigerian Criminal Law which states that a person convicted of fraud shall in addition to the term of imprisonment refund the stolen money or forfeit any property to which it has converted to the bank, financial institution or customer.

Under the Act, any person who uses any computer system or network for producing, distributing, procuring or transmitting child pornography is guilty of an offence punishable with 15-25 years' imprisonment.[21]This provision serves as a means of protecting children who aren't of legal age having their nudity shared with the whole world which might attract certain consequences in the future. It is immaterial whether the child's consented or not.

Section 18 of the Act makes it an offence for any person to access or cause to be accessed any computer or computer systems or networks for purposes of terrorism. The punishment for this offence is life imprisonment. The Act also makes provision for the punishment of persons who uses the internet to bully, threaten, insult, annoy, harass, share false information and cause enmity, hatred, ill will or needless anxiety to another.[22] The act recognizes this offence as Cyber stalking. The Cybercrimes Act also recognizes the offence of Cyber Squatting under Section 25. It provides that a person is guilty of Cyber-squatting if he intentionally takes or makes use of a business name, name, trademark, domain name or any word or phrase registered and owned by an individual, government, or body corporate without permission with the intention of interfering with their use by the owner. This offence is punishable with 2 years' imprisonment and #5,000,000.00 fines.[23] Section 32 of the Act makes it an offence to be engaged in phishing and spamming and the spread of computer viruses. Phishing is the act of fraudulent means of acquiring sensitive information such as usernames, passwords and credit card details through the e-mails or instant messaging system from banks or financial institutions. There exists plethora of provisions under the Cybercrimes Act which regulates the use of the Cyberspace. The Act specifies offences and prescribes punishment. This makes the Act the most suitable and novel legislation in the protection of users of the internet

[16] See Part of the Cybercrime (Prohibition, Prevention, etc) Act, 2015

[17]Section 3, ibid reads; ' the President may on the recommendation of the National Security Adviser, by order published in the Federal Gazette, designate certain computer systems, and or networks whether physical or virtual and or the computer programs, computer data and / or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating effect on the security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.'

[18] Section 5 ibid; The Act goes further in the interpretation section to define Critical Infrastructure as systems and assets, which are so vital to the country that destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country, section 58 ibid

[19] Section 6 (1) of the Cybercrime (Prohibition, Prevention, etc) Act, 2015

[20] Section 6(2) ibid

[21] Section 23 ibid.

[22] Section 24 ibid

[23] Section 25(1) ibid

in Nigeria. We shall however consider certain provisions of the Act that appear to be contrary to the provisions of the constitution especially with regard to the fundamental rights of citizen to freedom of privacy and expression.

Provision of Cyber Law that infringes on freedom of expression

Section 6(1) of the Acts, made a wide and sweeping provision prohibiting acts of espionage. While the objective of this provision and good intend is laudable, it is submitted that the wide and general prohibition of the acts of espionage will hinder Investigative journalism. This is because the section requires that journalists seek authorization before assessing any computer system or network and the attempt to access computer system or network without such authorization amount to 'fraudulent purposes' which is criminalized under the Act. Further, section 24 of the Act which criminalizes offensive and annoying statements on the internet appears to be an infringement of the rights of expression. The section prohibited cyberstalking and prescribes punishment of a fine ranging between NGN 7 million and 25 million, as well as imprisonment ranging between one and ten years, depending on the severity of the offence. Part of the provision of section 24 of the Cybercrime Act is reproduced hereunder:

> (1) Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that-
> (a) is *grossly offensive, pornographic or of an indecent, obscene or menacing character* or causes any such message or matter to be so sent; or
> (b) *he 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 or causes such a message to be sent: Commits an offence under this Act...
> (2) Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network –
> (a) To bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm or to another person;
> (b) *containing any threat to kidnap any person* or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value; … (Italics mine)

The above provision of the Cybercrime Act has been largely criticized by many Nigerians including legal practitioners. The criticisms centre on the argument that the provision is a violation of the right to freedom of expression entrenched in the Nigerian Constitution. The issue in the minds of many people, especially journalists, bloggers and online news sites, is the implications of these provisions of the Cybercrimes Act, its definition of 'Cyber stalking' and its implications on the constitutionally guaranteed freedom of expression and the freedom of the press as provided for in section 39 of the 1999 Constitution as amended.[24] This is because articles that are posted in mainstream newspapers and transmitted through the online portal of the publication or any other online platform and are deemed 'inflammatory,' 'obstructive' 'insulting' or 'aggressive' are actionable under this Act. Interestingly, even an objectively truthful story can be regarded as 'annoying,' 'insulting,' 'obstructive' or 'negative.' For example, section 24 (1) (a) prohibits the sending of obscene, pornographic or indecent messages through the internet. Whereas section 23, which criminalized child pornography is proper and accepted in order to protect public morality, however, with respect to section 24(1)(a) it is submitted that communication of pornographic or offensive messages between and among consenting adults should not amount to a crime.

Also with respect to subsection 2(a) and (b) thereof which prohibited the transmission of any communication through the computer system or network to bully, threaten or harass another; it is submitted that the failure of the Act to define or explain what amount to 'bully', 'Threaten' or 'harass' makes the provision opaque and therefore likely to place the ordinary citizen in a precarious situation. This is because the decision as to communication that amounts to 'bully', 'threaten', harass etc. is left to the law enforcement agencies and the court. The over-zealous law enforcement agents in Nigeria will readily arrest ordinary Nigerian citizens on the flimsy reason that the communication they made through the internet was capable of causing harassment, or was threatening or bullying. It therefore appears as if the Act was meant to protect the political class from public censorship or criticism. This same conclusion could as well be applied to section 24 (b) Which prohibits any person from knowingly sending a false message by means of a computer system or network for the purpose of causing annoyance, inconvenience, danger, obstruction, insults, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety. This provision appears to be nebulous and Draconian. First is the challenge of how to determine whether a message is insulting, or annoying or inconveniencing. Another is the question as to whether the fact that a message is

[24] E. Odeh , 'Cybercrime Act and Freedom of the Press in Nigeria.' <https://ijsser.org/2022files/ijsser07128.pdf> Accessed 17 December 2022.

annoying, inconveniencing or insulting will constitute enough reason or basis for the arrest and prosecution and eventual conviction and punishment of the sender of such message. In a society where citizens are bullied by the police, it is submitted that such provisions will give more room to police persecution as citizens can be arrested for just expressing themselves.

The provision of the section 24 of the Cybercrime Act has even been challenged in both the Nigerian courts and the ECOWAS court of justice. In the case of *Solomon Okedara v A.G. Federation*,[25] the Court of Appeal in Lagos dismissed a challenge to the constitutionality of Section 24(1) of the Cybercrime Act, 2015 on the ground that it lacked merit.[26] Affirming the judgment of Buba J. of the Federal High Court, the Court disagreed with the Appellant that the provision was vague, overbroad and ambiguous and threatened his rights to freedom of expression under Section 39 of the Constitution and was not within the permissible restrictions pursuant to Section 45 of the Constitution. Instead the Court of Appeal found Section 24(1) of the Cybercrime Act to be clear and explicit and not in conflict with the provisions of Sections 36(12), 39 and 45 of the 1999 Constitution. The Court equally rejected the Appellant's argument that section 24 of the Act does not satisfy the requirements of section 36(12) of the Constitution holding that in its view the words in section 24(1) of the Act are 'explicit and leave no room for speculation or logical deductions.' In a similar stand, in Suit No FHC/L/CS/692/16 at the Federal High Court,[27] the applicant sought declarative reliefs nullifying Sections 24 and 38 of the Cybercrime Act. The Court dismissed the application of the applicant and upheld the constitutionality of the section 24 and 38 of the Cybercrime Act. Dissatisfied with the decision of the Court, the applicant immediately appealed. The appeal was dismissed on June 1, 2018 by the Court of Appeal.[28] The case was further appealed to the Supreme Court and the court is yet to give a final verdict over the matter. We are hopeful that the Supreme Court will take a view contrary to that of the courts below.

It is worth mentioning that these cases are in pari material to the Indian case of *Shreya Singhal v. Union of India*[29] where section 66A (similar to section 24 of the Cybercrime Act) was declared void by the Indian Supreme Court on the ground that its wordings were vague. This same position was adopted by the Kenyan case of *Geoffrey Andare v. AG*[30] where the court declared section 29 of the Kenyan Act as unconstitutional for being vague and broad. On a positive note, the ECOWAS Court in a suit filed by SERAP ruled that section 24 of the Nigerian Cybercrimes Act violates Article 9 of the African Charter on human and People's rights and the Article 19 of the ICCPR.[31] The Regional court further ordered the Nigerian government to amend the section to ensure conformity with Nigerian's obligation under the ACHPR[32] and the ICCPR. It is submitted that the decision of the ECOWAS Court is a laudable one. While child pornography should rightly be prohibited, adult pornography should be a free choice of adults especially when viewed from the perspective that it does not violate any international law. However, where adult pornography may be posted to the internet by an adult, such material must contained prior warning to potential viewers.

Provision of Cyber Law that Infringes on Privacy Rights[33]

Section 7 of the Act requires that cyber operators maintain a register of users through a sign- in Register. This requirement is offensive to the right of privacy of citizens. Also, Section 38 of the Act makes provisions for the release of personal data of citizens in the possession of service providers at the request of relevant authority while Section 39 of the Act gives the judge the Authority to intercept electronic messages required for the purpose of criminal investigation or proceedings.

Section 38(2) of the Act provides as follows:

> A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section *or any law enforcement agency* –
> (a) Preserve, hold or retain any traffic data, subscriber information, non-content information, and content data; or

[25] CA/L/174/18 (unreported.

[26]<https: //globalfreedomofexpression.columbia.edu/cases/okedara-v-attorney-general.>accessed 6 December 2022

[27]unreported

[28]

[29]AIR 2015 SC 1523

[30] (2015)

[31]

[32]The African Union in 2002 adopted the declaration of the principle on freedom of Expression and Access to information in Africa. This declaration was updated in 2019 to include digital rights.

[33]Suit no. ECW/CCJ/APP/53/2018, JUDGEMENT No. ECW/CCJ/JUD/16/20 THE INCORPORATED TRUSTEES OF LAWS AND RIGHTS AWARENESS INTIATIVES V. FRN; https://cpj.org/wp-content/uploads/2020/09/nigeria-judgement_07-10-2020.pdf> accessed 17/05/23, See also Premium Times- March 28, 2022

> (b) Release any information required to be kept under subsection (1) of this section.
> (3) *A law enforcement agency may, through its authorized officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply*. (italics mine)

Further section 39 of the Act provides as follows;

> Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a judge may on the basis of information on oath:
> (a) order a service provider, through the application of technical means to collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or computer system.
> (b) Authorise a law enforcement officer to collect or record such data through application of technical means.

While we applaud the requirement of section 38 which impose a duty on service providers to keep traffic data and subscribers' information as it will enable the government in the fight against terrorism. We submit however, that contrary to the provision of section 38 (2) (b) that such data should only be released to law enforcement agency subject to the authority of the court of law.

On the provision of section 39 of the Act, the Act defines 'electronic communication' that could be intercepted to include communication in electronic format, instant messages, short message service (SMS), e-mail, video, voice mails, multimedia message service (MMS), fax and pager.[34] The Act further define 'interception' to includes 'listening to or recording of communication data of a computer or acquiring the substance, meaning or purport of such and any acts capable of blocking or preventing any of these functions'.[35] However, this provision violates the provision of Section 37 of the 1999 Constitution as amended which guarantees rights to privacy of individuals. The courts have also recognized and enforced this right.[36] In as much as the Act is desirable to fight cybercrime and terrorism as it is being done globally, there is a need to balance national interest with citizen's rights especially as there is a tendency for such a law to be abused by security agents. This was also the position of the courts in the case *Dasuki v. Federal Republic of Nigeria.*[37] In the case of *Incorporated Trustees of Paradigm Initiative for Reformation Technology Development & 2 ors v. AG Federation & 2 ors* the applicant challenged among others the constitutionality of section 38 of the Act on the ground that it infringes on the section 37 of the Constitution of the Federal Republic of Nigeria on privacy rights. The court however held otherwise. It is submitted however that the Act be amended to vest power on the court such that any regulatory authority who must access private information of a citizen must show justifiable cause why the court may allow it access to such private information.[38] The act by law enforcement agents of arresting, seizing laptops and cell phones of citizens especially young men without lawful order or warrant for the search or seizure of these properties, on the bogus excuse of searching for 'yahoo boys' amount to an infringement on their privacy rights. In the US case of US v. Arnold[39] a laptop computer, a separate hard drive, a computer memory stick and six compact discs were found on the defendant's bag and baggage. When the court was called upon to decide whether the government can access stored information in the digital devices in the absence of a search warrant, the court held that evidence derivable from an individual's private portable storage devices must be subjected to a search warrant and in the absence of such the evidence there from is suppressed[40] these decision followed an earlier case of Steve Jackson Games, Inc. v. United States Secret Service.[41] Where the US court held that a search warrant was required for lawful search and seizure of computer software, computer hardware, electronic mail, and stored electronic communications. Thus it is contended, that since an individual has a reasonable expectation of privacy, a warrant disclosing grounds for

[34] Section 58 of the Act.
[35]Ibid
[36]See the case of Solomon Okedara v. Attorney General of the Federation n*58*
[37] (2016) ECW/CCJ/JUD/23/16.
[38]Example is where access to such information or data is necessary for the facilitation to criminal investigation. See T. F. Govender (2018), Acritical Analysis of the Search and Seizure of Electronic Evidence relating to the Investigation of Cyber-crime in South Africa. LLM Thesis university of KwaZulu- Natal, 18, 33,
[39](2006)
[40] B. A. Stiwagon, (2008) Bringing an end to Warrantless Cell Phone Searches, Georgia Law Review, 42(4)1175-1177
[41](1994)

probable cause is required before a law enforcement agent can access the text messages or emails of persons subject to investigation.[42]

Finally, section 40(2) requires that service providers assist law enforcement agents either on the request of the law enforcement agents or on the personal volition of the service provider and further made failure of a service provider to do so a punishable offence. We submit that why it is proper for service providers to assist law enforcement agencies, such assistance shall be on the request of the agencies and not on the personal volition of the service provider, especially as the Act made failure to do so a crime. Therefore, the clause 'On his own initiative' should be expunged Such that service providers will be mandated to provide such assistance on the request of law enforcement agents.

3. Conclusion

This article has shown that the Nigerian government in response to the negative impacts of the ever growing use of the cyberspace to carry out criminal activities enacted the Cybercrime (Prohibition, Prevention, etc) Act, 2015. It applauded the enactment of this Act as it demonstrated the government commitment to confront the different forms of offences committed against and through the computer system and the internet. However like any other new piece of legislation aimed at curbing a new form of deviant behaviour in a society, this legislation have been confronted with the challenges of balancing the need to stamping-out criminal activities and that of protecting national security and individual privacy of citizens and also the equally most important need of preserving and promoting the fundamental rights of citizens to freely express themselves without state interference as well as their rights to privacy of their persons, homes and correspondence. We have identified specific provisions of the Act that runs afoul of citizens' rights to freedom of expression and privacy and have recommended amendment of the offending sections. We have recommended the amendment of section 6 (1) by including a proviso exempting registered journalist from liability under the section. Also we recommended the deletion of section 24 (2)(a) of the Act since a mere verbal threat should not be criminalized. Further, section 24(b) ought to be expunged from the Act for being vague. With respect to section 38 and 39 of the Act it is advocated that the powers of the law enforcement agency under the section be subjected to the review jurisdiction of the court of law. This is because the powers vested on the law enforcement agencies under the section will impact on the right of citizen to privacy. Finally, with respect to section 40(2) we recommend the deletion of the expression; 'at its own initiative'. It is believed that with the recommended amendment, the Act will in turn be well positioned to curb the menace of cybercrime as well as safeguard the rights of citizens against intrusion and surveillance. In all the cybercrime has come to stay as part of Nigerian law. Cyber criminals will continue to develop new strategies and method of carrying out their nefarious activities. To meet up with the challenges of combating cybercrime, our legislators must continue to be innovative and broadminded in order to continue to effect the necessary modifications to the Act as and when needed.

[42]D. J. Waxse (2016) Search Warrant for Cell Phones and Other Locations Where Electronically Stored Information Exists: The Requirement for Warrants Under the Fourth Amendment, Federal Courts Law Review, 9(3)1-4