LEGALITY OF THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT AS AN INSTRUMENT FOR INTERNET CRIMES CONTROL IN NIGERIA.

Somtochukwu D. Ojukwu[*]
Obianuju C. Agu[**]

Abstract

As the rate of Internet use rises across the world, there has also been a concomitant rise of abuse in its use. Abuse has become rampant as Internet offers near unrestricted accessibility and is designed to work without the kind of gatekeepers that exist in traditional media of communication. This situation has raised concerns at the national and international levels of governance, necessitating the enactment of specific statutes and instruments for the regulation and control of Internet crimes. Nigeria is one of the countries that has specific legislation on Internet crimes with the enactment of Cybercrimes (Prohibition, Prevention, Etc) Act which creates strict standards in the use of Internet as well as offences which are specific to use of Internet and electronic devices in general. This work made a critical review of the position of the law on the legality or otherwise of the Act, making reference to decisions of the courts in cases where the constitutionality of the Act has been challenged in courts.

Key words: Internet, cybercrime, Nigeria Cybercrimes Act,

1. Introduction

Globalization has made the use of Internet[1] imperative and a necessity in all spheres of human activities and existence. Today, information and communication technologies (ICTs) are omnipresent and the trend towards the use of Internet is growing, even in areas that usually function without computer. The world has experienced a leap in the request and use of Internet facilities, irrespective of age and gender. Internet connects millions of computers together globally, forming a network in which any computer or device can communicate with the other as long as they are both connected to the Internet. On the Internet, users are not mere consumers of content but also creators of content. Therefore, it is a means of communication which allows individuals to express their opinions directly to the world audience, while allowing them access to other ideas and information from or by others. It has afforded the infrastructure for development in the creation, availability and use of network-based services. For instance, E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communications like WhatsApp, Facebook calls are becoming more used than the conventional network calls.

[*]**SD Ojukwu**, Lecturer and postgraduate scholar, Faculty of Law, Nnamdi Azikiwe University, Awka, somtoojukwu@gmail.com.
[**]**OC Agu**, Lecturer and postgraduate scholar, Faculty of Law, Nnamdi Azikiwe University, Awka, uju.agubosim@gmail.com.

[1] The words, 'Internet' and 'Cyber' are used interchangeably as it suits

Following the above, Internet affords a platform for many activities which require transfer or exchange of information. Being a platform for exchange of information, it has been a breeding ground for unlawful activities generally described as cybercrimes[2]. The growth in Internet crime is becoming proportional to the growth of the Internet itself, and so is the variety of these crimes called cybercrimes and other Internet abuses being committed or attempted.[3]Whilst the Internet has helped many organizations and individuals attain global recognition, the wrong use of the Internet can also cause harm and even make businesses go extinct. A study by the security firm McAfee and the Centre for Strategic and International Studies (CSIC) also revealed that cybercrime has cost the global economy almost of $600 billion annually and is the main contributorfor dragging down economic growth across the world.[4] In 2018, the United States Federal Bureau of Investigation (FBI) received a total of 351,936 complaints on Internet fraud with losses exceeding $2.7 Billion.[5]Although countries like the USA and Britain have recorded billions of dollars and pounds respectively in losses to Cybercrime, Nigerian is not an exception. In 2016, the Federal Government said the estimated annual cost of cybercrime to Nigeria is 0.08 per cent of the country's Gross Domestic Products (GDP), which represents about N127 billion.[6]

According to Ashaolu and Oduwole,[7] cybercrime, has collapsed and literally paralysed consumer confidence in e-commerce. Many people avoid trading online because of concerns about the integrity of the Internet and fears that personal details such as credit card data and other confidential information might be compromised. These figures clearly demonstrate the importance of protecting information infrastructures by all means.[8]The cost of cybercrime to any nation is enormous and can completely ruin the country's economy if the proper security strategies are not put in place. Hence, the need for intervention in this sphere to control the activities done online to avoid an upsurge of Internet crimes. The governments of the world are continuously carrying out research to

[2]Other unlawful Internet activities include cybersquatting, cyberstalking, phishing, cyberterrorism, cybertheft, cyber warfare, cyber espionage

[3] K. Nandan, 'Law Relating to Computers Internet and E-Commerce' (5th Edition, India: Universal Law Publishing Co. Pvt. Ltd., New Delhi, 2014) pp. 208 - 209

[4] James Lewis, 'Economic Impact of Cybercrime-No Slowing Down', (Mcafee, Feb 2018) <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf> accessed 17th July 2020

[5] Federal Bureau of Investigation (FBI), 2018 Internet Crime Report. <https://pdf.ic3.gov/2018_IC3Report.pdf.> accessed 12th August 2020

[6] Nigerian Communication Commission, 'Final Report on: Effects of Cybercrime on Foreign Direct Investment and National Development,' p. 15 <https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file> accessed 10th August 2020

[7] D. Ashaolu and A. Oduwole "Policing Cyberspace in Nigeria, a publication in honour of Col. Sani Bello (Rtd) (Nigeria: Life Gate Publishing Co. Ltd, Ibadan, 2009)

[8] G. C. Wilshusen, 'Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan', Testimony before the Subcommittee on Information Policy, Census, and National Archives House Committee on Oversight and Government Reforms (United States Government Accountability Office, GAO-08-212T, 2007) <www.gao.gov/new.items/d08212t.pdf> accessed 10th August 2020

improve their cybercrime attacks counter-measures. Consequently, Nigeria has the Cybercrimes (Prohibition, Prevention, ETC) Act which was made specifically to control Internet activities against cybercrime.[9]

2. Meaning and Nature of Cybercrimes

The open nature of Internet as well as its geographical limitlessness implies that Internet provides a fertile ground for criminal activities collectively referred as cybercrime. The term 'cybercrime' may not be capable of a definite definition for many reasons, including the dynamic nature of the acts that constitutes cybercrime. It is however used to cover a wide variety of criminal conduct that is perpetuated using computer with Internet access.[10] According to Nigerian Communication Commission, cybercrime may generally be regarded as criminal offence involving a computer as the object of the crime (hacking, phishing, spamming), or as a tool to commit a material component of a crime (child pornography, hate crimes, computer fraud)[11] In simple terms, cybercrime may be explained as crime committed using the Internet. It is used to describe a range of offences including traditional computer crimes, as well as network crimes.

Two approaches have been given in the definition of cybercrime at the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders.[12] These are cybercrime in a narrow sense (computer crime) which covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them and cybercrime in a broader sense which covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[13] Therefore, cybercrime covers offences involving cyberspace, computers and other electronic information storage devices, such as data interference, illegal interception, illegal access and the misuse of devices.[14] Some definitions try to take objectives or intentions into account and define cybercrime more precisely, such as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.

[9]The Cybercrimes Act is made up of 59 Sections, 8 Parts; and 2 Schedules.
[10] Some of the most well-known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography.
[11] Ibid. Footnote 6
[12] Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders' (A/CONF.187/10 April 2000).
<https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf> accessed 16th August 2020.
[13]Ibid. Footnote 11
[14] K.S. Chukkol, 'The Law of Crimes in Nigeria' (Ahmadu Bello University Press Ltd, Revised Edition 2010)

Another approach in understanding cybercrime can be through the deciphering of words making up the concept. Cybercrime or computer crime has two elements, "Computer" and "Crime". Therefore, it involves a crime in a relationship with a computer. The relationship could involve the direct usage of computer by the cybercriminal as was the first recorded instances of cybercrime. It may as well be indirect where the cybercriminal many not only use a computer to commit crime but may make changes in a computer system by manipulating a key computer user. Thus, one being the exploitation of weakness in the technical IT infrastructure, and the other being exploitation of trust in social fabric of IT users, within the organization.

Some scholars have argued that the prevention and remediation of cybercrime hinge on definitional clarity[15], defining cybercrime and creating a distinction between cybercrime and other malicious activities may only be beneficial for creating specific policies on combatting the ever expanding range of cyber threats. It is therefore pertinent in dealing with cybercrime to focus more on the specific threats and legislate on them instead of throwing the criminalization of an activity to a single definition where intelligent people can easily commit a moral wrong with the defence that it does not fall under the definition of cybercrime.

Also, some have criticized the categorization of cybercrime. Gotternbarn argued that, there is nothing special on the crimes that happen to involve computers. Is it possible for a crime being categorized in accordance to a tool, equipment, mechanism or means through which it was committed? If that's so, how many categories of crime would be there? How about the crime committed through using a television, automobiles, scalpels, scissors and other tools, can we categorize each of them as individual crimes?[16]Gotternbarn concludes that crimes involving computers are not necessarily issues in computer ethics.

Unfortunately, most statutes and instruments related to cybercrime do not provide a definition of it. Following the above definitions, cybercrime involves a three-stage classification, as summarized by the US Department of Justice noted that the definition of cybercrime involves a three-stage classification:

1. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attack.
2. Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement, fraud and forgery offences.
3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the

[15] S. Gordon and R. Ford, 'On the Definition and Classification of Cybercrime," (Vol. 2, July 2006) *Journal of Computer Virology*, pg 13

[16] T. T. Herman, 'Ethics and Technology, Ethical Issue in an Age of Information and Communication Technology', (2nd Edition, Hoboken, NJ: Wiley, 2007) P.20

> computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more a repository for evidence.[17]

Another approach can be found in the Convention on Cybercrime,[18] which distinguishes between four different types of cyber offences:

1. offences against the confidentiality, integrity and availability of computer data and systems;[19]
2. computer-related offences;[20]
3. content-related offences;[21] and
4. copyright-related offences.[22]

Cybercrime through abuse of information infrastructure and Internet services have the potential to harm society in new and critical ways. Online fraud and hacking attacks are just some examples of cybercrimes that are committed on a large scale every day using Internet facility that is meant to impact positively on the society. The financial damage caused by cybercrime is reported to be enormous.[23] In view of the enormous economic and social loss that the abusive use of Internet could perpetuate, there is an obvious need for cyber control or regulation. Cyber regulation can be in various forms. For example, a country might see some social media websites/platforms as a national threat thereby restricting citizens' access to such sites/platforms. It could be obligation on Internet Service Providers to keep record of access to Internet through their service etc. These are all geared towards maintaining the sanctity of the Internet sphere.

3. Inadequacy of General Criminal Statutes to Combat Cybercrime

Prior to the assent of Cybercrimes Act in 2005, the statutes on criminal law were relied on in the efforts to regulate Internet and consequently control cybercrime in Nigeria.[24]This reliancewas fraught with many *lacuna* as these dated criminal statutes were made without anticipation of the nature and complexity of cybercrime. It is to be noted that the existing Criminal Code laws and Penal Code laws where made prior to the level of development of Internet criminal activities experienced today. Also, use of

[17] Jonathan Clough, 'Principles of Cybercrime', (1st Edn, Cambridge University Press, 2010) 27.
[18] Council of Europe Convention on Cybercrime (CETS No. 185), http://conventions.coe.int. accessed 8th June 2020
[19] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices).
[20] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud).
[21] Art. 9 (Offences related to child pornography)
[22] Art. 10 (Offences related to infringements of copyright and related rights)
[23] CS Ibekwe, GC Oko, Emerging Issues in Copyright Protection Law for Digital Innovations in Nigeria, (2020) 2(1) *IRLJ*, 117.
[24]These statute include Criminal Code, Penal Code, Advanced Fee Fraud and other Related Offences Act, Money Laundering Act

Internet and Internet crimes are rapidly developing in dimensions not covered by these mentioned statutes, leaving these laws obsolete in the bid of controlling Internet crimes. It is a cardinal principle of criminal law that a person cannot be convicted for an offence that is not stipulated in a written law in which the penalty for the offence is clearly spelt out.[25] Therefore, for an action to be a criminal offence, a written law must prescribed a punishment for the doing of the act. In the instance, the Criminal Code and Penal Code does not adequately provide for offences related to Internet. The Criminal and Penal Code does not address areas or envision issues like the jurisdiction bearing in mind that Internet crimes are often extra-territorial as it can be committed outside Nigeria by Nigerian or committed by a non-Nigerian outside Nigeria but with its victim being a Nigerian and resident in Nigeria. Cybercrimes Act came as a child of necessity to harmonize and cover the lacuna in criminal law by criminalizing certain acts as cybercrime, resolving issues of jurisdiction. It also addressed issues of investigation and evidence in cybercrime matters.

The Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 provides a comprehensive and principal enactment for the regulation and control of activities of Internet as an effective tool for minimizing Internet crimes. It provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria, which is aimed at promoting cybersecurity, computer systems and networks.[26] The Act ensures the protection of critical national information infrastructure and promotion of cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights in Nigeria.[27]

Apart from criminalizing certain acts, prescribing punishments for their commission and creating an institutional and enforcement framework, the Cybercrimes Act addresses most of the lacunae which had hitherto rendered the Nigerian cyberspace unsafe for transacting business.

4. Constitutionality of the Cybercrimes Act

The question on the constitutionality of Cybercrimes Act in a good part stems from the issue of legality of the National Assembly to enact law on cybercrime when cybercrime is not listed in the Exclusive Legislative List. The legislative power of the National Assembly is under the strict regulation of the express provisions of the Constitution from which the powers are derived.[28] This means that any law made by the National Assembly outside their legislative power in the Constitution is ultra vires.[29]

[25] CFRN, S. 36(12)
[26] Cybercrimes Act, Section 1 which stipulates the objective of the Act
[27] Explanatory Memorandum to Cybercrimes Act
[28] CFRN, S. 4(2), (3) and (4); SRN Plc v. CBN (2009) 6 NWLR [pt. 1137] 287.
[29] AG Abia State v. AG Federation (2006) 16 NWLR [pt .1005] 265

Cybercrime is neither listed in the Executive Legislative list nor Concurrent Legislative list which leaves us with a position that cybercrime is of residual list, in which case the National Assembly is excluded from legislating on it. The Exclusive List contains 68 items which the National Assembly is empowered to legislate.[30] However, as already highlighted above, cybercrime has become a rampant act in Nigeria, which has caused government, businesses and Nigerian citizens so much fortune and reputation to an extent it can safely be assumed that it threatens the peace and unity of Nigeria. In *Odiawa v. Federal Republic of Nigeria*[31], the Court of Appeal said that cybercrimes are serious offence which is heinous as armed robbery. Following the position taken by the Court in the above referred case, it can be said that cybercrime poses a threat to peace, order and good governance of Nigeria. The National Assembly is empowered by the Constitution[32] to make laws for the peace, order and good governance of the Federation.[33]

In the case of *Attorney General of Ondo State vs. Attorney General of the Federation &Ors*[34], the government of Ondo State brought an action at the Supreme Court, seeking a determination of the question whether the National Assembly has the power to enact Corrupt Practices and other related Offences Act.[35] The Ondo State government argued that "Corruption" is not specifically mentioned in the Exclusive List and therefore the National Assembly cannot legislate on the subject of corruption. It was further argued that "Corruption" is also not in Concurrent List and therefore, is implied to be in Residual List which the National Assembly cannot make legislate on. In the determination of the case, the Supreme Court held that the National Assembly has the legislative competence to legislate on corruption and the argument of the government of Ondo State is advanced without the government taking in to cognizance the provisions of S. 4(4)(b) of the Constitution which provides that the National Assembly has power to legislate on any matter with respect to which it is empowered to make law in accordance with the provision of the Constitution. Particularly, Ogwuegbu JSC held as follows:

> Section 4(2) of the Constitution conferred on the National Assembly power to make laws for the peace, order and good government of the federation or any part thereof with respect to any matter included in the exclusive legislative list set out in part 1 of the second schedule of the constitution. Section 4 of the constitution recognizes the need for the peace, order and good government in relation to Nigeria as a nation just as it recognizes the need for peace, order and good government in relation to each separate of the federation hence it conferred power on the National Assembly to enact laws to achieve that objective. Corrupt

[30] CFRN, Part I, 2nd Schedule
[31] (2009) LPELR-4230 (CA)
[32] CFRN, S. 4
[33] CFRN, S. 4(4)(b)
[34] (2002)9 NWLR [Pt. 772] 222
[35] ICPC Act 2000

> practices and abuse of power can, if not checked threaten the peace, order and good government of the federation or any part thereof… I have held in this judgment that the National Assembly can exercise the powers which it does not possess for the purpose of assisting in carrying out a policy which may affect matters which are directly within its legislative competence. It can also exercise powers, which it does possess for assisting in carrying out a policy, which may affect matters not directly within its legislative powers

Adopting the *ratio decidendi* of the Supreme Court on the Ondo's case which is similar to the issue presently considered, it is safe to state that the National Assembly has the constitutional right and therefore validly enacted the Cybercrimes Act. Despite the fact that cybercrime is not expressly listed in the Exclusive List nor the Concurrent List, there is good cause to submit that the National Assembly has the legislative powers to make laws on cybercrime and that the Cybercrimes Act is constitutional and enforceable in Nigeria.

4.1 Judicial Challenges on the Constitutionality of Provisions of the Cybercrimes Act

As discussed above, the National Assembly has the powers to make Cybercrime Act. However, there has been to some provisions of the Act for the reasons of being in conflict and inconsistent with the Constitution and accordingly, should be null and void, at least to the extent of its inconsistency.[36] In *Solomon Okedara vs. Attorney General of the Federation*[37]the Appellant, as Plaintiff at the Federal High Court[38], challenged the validity of S. 24 Cybercrimes Act and prayed the court to nullify same on the ground that it violates S. 36 (12) and 39 of the Constitution. The Appellant contended that S. 24 Cybercrimes Act is illegal, unconstitutional and in violation or likely to further violate the Appellant's fundamental right to freedom of expression and the press guaranteed by S. 39 of the Constitution. Particularly, the Appellant argued that the S. 24 impedes on the right to give and receive information and freely express ideas.

The contested provision of S. 24 Cybercrimes Act particularly provides for the offence of cyberstalking which it described as when a person sends a message via computer that is grossly offensive, menacing, obscenely indecent, criminally intimidating, or false with the aim of causing needless anxiety, insult, danger, obstruction, threat to kidnap/request for ransom/ kidnapping, hatred, harassment, bullying, violence, bodily harm or death. The S. 24 Cybercrimes Act provides thus:

> 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 an indecent or menancing character or causes any such message or matter to be sent; or

[36] CFRN, S.1(3)
[37] (2019) LPELR-47298(CA),
[38] Before Hon. Justice I. N. Buba

> 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 and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

The court in the case recognized without any doubt that under the 1999 Constitution, liberty of thought and freedom of expression is paramount. It also stated clearly that the provisions of S. 39 of the Constitution are clear and unambiguous to the effect that it guarantees that every citizen of this country shall be entitled to freedom of expression which was extended to include the freedom to hold opinion and pass information without interference. This freedom presupposes free flow of opinion and ideas essential to sustain the collective life of the citizenry. It however stressed that it is very important to know that the right provided under Section 39 is not an open-ended or absolute right; the right is qualified, and therefore subject to some restrictions and derogations by the provisions of S. 45 of the Constitution.

The Appellant in the case also made an argument that that the offense created by S. 24 Cybercrimes Act was overbroad and vague. The trial court[39] reasoned that the provision was not vague, that cybercrime is incapable of direct definition and that the restriction on freedom of speech was necessary in a democratic society in the interests of defense, public safety, public order, public morality or public health pursuant to section 45 of the Constitution. The Applicant being dissatisfied with the decision of the trial court appealed the judgment. The Court of Appeal[40] on 28th February 2019 unanimously dismissing the appeal and upholding the judgment of the trial court held that the S. 45 provides that nothing in S. 37, 38, 39, 40 and 41 of the Constitution, shall invalidate any law that is reasonably justified and which is made on the interest of public defense, public safety, public order, public morality, public health or for the purpose of protecting the rights and freedom of other persons.

The Court relying on the above upheld the provisions of S. 24 Cybercrimes Act as constitutional, not being in conflict with S. 36 (12) and 39 of the 1999 Constitution. The Court of Appeal in its own judgment expressed the same position that the legislature has the power to enact laws that are reasonably justifiable in a democratic society and such laws shall not be declared invalid merely because they appear to be in conflicts with the rights and freedom extended to citizens under the Constitution. It went further to hold that it is within the powers of the legislature, in the interest of the public, to place restrictions and introduce safe-guards upon the constitutional right of a citizen. Therefore,

[39] Per Justice Buba who was sitting at the Federal High Court
[40] Per Tijani Abubakar JCA, Abimbola Obaseki-Adejumo JCA, Jamilu Tukur JCA

the right of freedom of speech guaranteed under Section 39 is subjected to the purposes of preserving the interest of defense, public safety, public order, public morality, public health or for the purpose of protecting the rights and freedom of other persons.

S. 38 Cybercrimes Act appears to be the most debated and controversial provision of Cybercrimes Act, as the constitutionality of the provision has severally been called to question and even challenged in court. The Act in this regard requires every service provider to keep all traffic data and subscriber information as may be prescribe by the relevant authority responsible for the regulation of communication services in Nigeria for a period of 2 years and at the request of the regulatory body or law enforcement agency, release such information. Any person that contravenes this provision shall be liable on conviction to a term of not more than 3 years or a fine of not more than N7,000,000 or to both fine and imprisonment. S. 38 Cybercrime provides:

> (1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being, responsible for the regulation of communication services in Nigeria for a period of 2 years.

In Incorporated Trustees of Paradigm Initiative for Preformation Technology Development & 2 Ors vs AG Federation & 2 Ors,[41]the constitutionality of Ss. 24 and 38 Cybercrimes Act was challenged at the Federal High Court. The Applicant made the same arguments as discussed above with respect to constitutionality of S. 24 Cybercrimes Act. On S. 38 Cybercrimes Act, the Applicant argued that the provision which require service providers to disclose online user data to law enforcement agencies does not only inhibit communication but violates freedom of expression guaranteed by S. 37 of 1999 Constitution. The trial court[42] cited the case of *Medical and Dental Practitioners' Disciplinary Tribunal v. Emewule& Anor*[43], in holding that fundamental rights are limited by state policy and overriding public interest and the right to private and family life cannot be an exception. The court went further to state that the provisions of S. 39 of the Constitution grants the right to freedom of expression and information, it also places condition precedent which protects other members of the society from defamation and false information. Based on the above, the trial court found the case lacking in substance and dismissed same.

On appeal[44], the Appellate Court held that S. 38 merely states what is universally accepted that any member of society must partner with law enforcement for an effective enforcement of criminal legislation. The Court of Appeal went further to state that the court is inclined to consider the objectives of Cybercrimes Act as contained in S. 1, the provisions of S. 38(5) of the Act. The Court held that based on S. 45 of the Constitution,

[41] FHC/L/CS/692/2016;
[42] Per Hon. Justice M. B. Idris delivered 20th January 2017
[43] (2001) 3 SCNJ 106
[44] CA/L/556/2017 (Unreported) delivered 1st June 2018

nothing in S.37-41 of the Constitution shall invalidate any law that is reasonably justifiable in a democratic society.

It would be most difficult to say that the S. 38 Cybercrimes Act is unconstitutional in view of S. 38(5) Cybercrimes Act which has taken into view the likelihood of conflict with s. 38 of the Constitution. S. 38 (5) Cybercrimes Act provides as follows:

> Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement

In view of the above, the constitutionality of S. 38 Cybercrimes Act does not need to arise as it has expressly provided that the provisions of S. 38 Cybercrimes Act is subservient and subject to the Constitutionally guaranteed right to privacy which must be protected by the service provider.

The position taken by the Nigerian Court may be different in other jurisdiction with strict command to preservation of fundamental right. In United States, the first major Supreme Court ruling on the regulation of materials distributed via the Internet is the case of *Reno v. American Civil Liberties Union*[45]. The case considers the American federal Communications Decency Act (CDA) which seeks to protect minors from explicit material on the Internet by criminalizing the knowingly transmission of obscene or indecent messages to any recipient under 18 years and also the knowingly sending to a person below 18 years anything that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs. The American Civil Liberties Union argued that certain parts of the CDA were facially unconstitutional and sought a preliminary injunction preventing the government from enforcing those provisions. In the landmark decision, the US Supreme Court unanimously ruling that anti-indecency provisions of the 1996 Communications Decency Act (CDA) violated the First Amendment's guarantee of freedom of speech and is unconstitutional.

5. Conclusion

It is a clear fact that Internet crime is vast and evolves along with changes in technology. This implies that cybercrime cannot be easily and completely eliminated, but can only be minimized through the collaborative efforts of individuals, corporate organization and government in bringing it to a minimal level. On the part of government, the Nigerian government through the enactment of Cybercrimes Act, seeks to regulate the use of Internet and electronic device in general as a means of controlling cybercrime.

[45]521 U.S. 844 (1997)

Cybercrime involves so many activities which is not contemplated by the general criminal statute. Therefore, the enactment of the Cybercrimes Act was necessary and to a large extent filled the lacuna which is created by the insufficiency of the general criminal statutes as it relates to cybercrime.

Although the Act created vital and notable legal frame work for cybercrime control, there has been a challenge on the constitutionality of the National Assembly to make the Act. Also, it has been a subject of court litigation whether or not certain provisions of the Act is void, being that they are inconsistent with the provisions of Constitution, particularly the fundamental rights of individuals. The Courts have intervened many times in this regard and have affirmed the challenged provisions of the Act as constitutional and an allowed derogation on the guaranteed fundamental right of individuals.

Even with the affirmation of the constitutionality of the Cybercrime Act by the courts, the Act is presently challenged as the rapid changes in complexity and forms of cybercrime is clearly threatening to leave it behind and make it obsolete. The amendment of the Act is therefore recommended in keeping pace with the changes in technology and the new modalities of cybercrime which were not contemplated by the Act.