LEGAL FRAMEWORK FOR THE ENFORCEMENT OF CYBER LAW AND CYBER ETHICS IN NIGERIA.

UMEJIAKU, NNEKA OBIAMAKA
Lecturer, Department of Commercial and Property Law
Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria.
E-mail:nnekaumejiaku@gmail.com

&

ANYAEGBU, MERCY IFEYINWA (Ph.D)

Faculty of Law Library,
Nnamdi Azikiwe University, Awka, Nigeria.
E-mail:ifymanyaegbu@yahoo.com

Abstract

Cyber law deals with codified rules that govern the exchange of communication and information for the protection of intellectual property rights, freedom of speech and public access to information in cyber space. Cyber ethics on the other hand is the application of responsible behavior on the Internet. Currently in Nigeria, the *Cyber Crime Act* was promulgated in 2015 to tackle online offences. This paper examined the legal framework which regulates public access to information in the cyber space in Nigeria. The paper also highlights lapses inherent in Nigerian legal system. Based on the findings, the paper proffers a number of recommendations. It also observes that due to rapid development in technology, law and ethics should be combined to protect the society from the menace of cybercrime.

Introduction

The need to combine ethics and law in regulating the activities of cyber world cannot be over emphasized. This is crucial in order to curb the menace of cyber crime which has eaten deep into the fabrics of the society. Information technology has made the world a global village and has enhanced every sphere and sector of the society like economy, commerce, social and educational sectors.

However despite the advantages, the society is threatened by the growing trend of cyber crime. Arguably, cyber crime thrives because of lack of universal legal framework and jurisdictional challenges that make it difficult to bring cyber criminals to book. For example, someone could be in Nigeria and commit a cybercrime that will have effect in South Africa and Canada respectively. The question that comes to bear is which jurisdiction will try him, will he be tried by South African law or Nigeria law. This challenge has exacerbated the criminal activities of cyber crime in the world especially in Nigeria where it has escalated due to unemployment.

The absence of international legal Framework to combat the activities of cyber criminals has threatened the security of the State. Nigeria in 2015 promulgated the *Cybercrime Act 2015* to curb the menace of cybercrime but the Act has failed to totally arrest the ugly trend because of some gap or lacuna in the Act and also due to so many other factors that exacerbate cyber crime in Nigeria. This work x-rayed the *Cybercrime Act 2015* and other legislations that have tried to combat cyber crime and also highlights those factors that have hindered positive changes in the cyberspace.

The paper reviewed the legal frame work in Nigeria and observed that none has been able to totally eradicate the menace of cyber crime. The writers are of the view that law alone is insufficient to tackle the menace of cyber crime. Due to increased technological advancement and new fraudulent devices of the cyber criminals, combined effort of both law and ethics will be a formidable tool to arrest the ugly trend and maximize the benefit of technological advancement in the information world. These efforts should not be left in the hands of the government alone. Every stakeholder in the information industry should join to win the war against and procure the security of the cyberspace and its users.

1. Cyber Law and Ethics

The need for the regulation of cyber world cannot be over emphasized because of the technological advancement which has transformed the world into a global village. Cyber law entails the safe and lawful collection, retention, processing, transmission and use of personal data of individuals. The need for cyber protection stems from legal models derived from a body of common rules such as the *United Nations Universal Declaration on Human Rights*[1] and the *European Convention of Human Rights* which provide for the right of every individual to privacy[2]. An instance of data protection legislation can be illustrated with the *European Convention on Human Rights* which provides for the right of respect to private and family life. It further provides that there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic wellbeing of the country? It also provides for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others[3].

However, with the advances in automation of data, respective countries of the world and some national bodies like the European Union, have made concerted effort to develop all-inclusive body of rules on data protection such as the *European Data Protection Directive and the Directive on Privacy and Electronic Communications* which incorporate principles that regulate the collection, retention, processing, transmission and use of personal data in the region.

[1] Universal Declaration on Human Right 1948
[2] European Convention on Human Rights
[3] Ademola Adeniyi, the Need for Data Protection Law in Nigeria httpas://adeadeniyi.wordpress.com accessed on 28/10/2015

2. Data Protection Principles

Under the *European Data Protection Directive, the Directive on Privacy and Electronic Communications*, and the *United Kingdom Data Protection Act*, certain principles are fundamental and they are universally agreed as "Data Protection Principles". They have formed the body of data protection laws all across major countries of the world, particularly in America and Europe. This body of principles regulates and ensures that personal data is collected, collated, processed, transmitted and transferred without infringing on the personal privacy of the individual. These principles include the following:

- personal data shall be processed fairly and lawfully.
- personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- personal data shall be accurate and, where necessary, kept up to date.
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- personal data shall be processed in accordance with the rights of data subject under this Act. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data should not be carried out of such countries if they do not have similar data protection laws and measures such as the European Union.[4]

[4] Ibid

3. The Need for Cyber Law and Cyber Ethics

Ethics generally refers to moral obligation that one person owes another[5]. It also refers to the standard of character set up by any race or nation[6]. Further, ethics refers to treating of morals in accordance with right principles as defined by a given system of ethics or professional conduct[7].Cyber ethics refers to the code of responsible behavior on the Internet. Responsible behavior on the Internet in many ways aligns with acceptable behavior in everyday life, but the consequences can be significantly different. Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society. In the late 19th century, the invention of cameras, spurred similar ethical debates as the Internet does today. During a *Harvard law Review* seminar in 1890, Warren and Brande defined privacy from an ethical and moral point of view to be central to dignity and individuality and person hood. Privacy is also indispensable to a sense of autonomy, a feeling that there is an area of an individual's life that is totally under his or her control, an area that is free from outside intrusion. The deprivation of privacy can even endanger a person's health. Over 100 years later, Internet and proliferation of private data through government[8] and e-commerce is a phenomenon which requires a new round of ethical debate involving a person's privacy.

Cyber ethics is distinct from cyber law. Laws are formal written directives that apply to everyone, interpreted by the judicial system and enforced by the police.[9] Ethics generally is the study of what is good for both the individual and

---

[5] Byran A. Garner, *Black's Law Dictionary* 9th Ed., Paul Minn. 2009.
[6] Albert .H. Mack Ward; the *New International Webster's Comprehensive Dictionary of the English Language*, Encyclopedic Ed., Trident Press International Florida. 2004.
[7] Ibid
[8] Warren .S, Brandeis. L."privacy, photography and the press" *Harvard Law Review*(1998)
[9] http://en.wikipedia.org/wiki/cyberethics

society. Ethics is a broad philosophical concept that goes beyond simple right and wrong, and looks towards the good life. Information technology managers are required to establish a set of ethical standards common to their organization. There are many examples of ethical code currently published that can be tailored to fit any instrument that establishes a common ethical framework for a large group of people.

From the foregoing definition one can say that cyber ethics involves the moral behavior on the Internet or in cyber space. Responsible behavior on the Internet in many ways aligns with acceptable behavior in everyday life, but the consequences can be significantly different[10]. While laws are formal written directives that apply to everyone, interpreted by the judicial system and enforced by the police[11].Ethics generally is the study of what is good for both the individual and society. Ethics is a broad philosophical concept that goes beyond simple right and wrong and looks towards the good life.

4. Origin of Computer Ethics

Computer ethics was discovered by Norbert Wiener in mid-1940s (a professor of mathematics and engineering at MIT) originally called cybernetics and include the following:

- Computer ethics deals with how computing professionals should make decisions regarding professional and social conduct.
- Who administrates the Internet
- Internet Society (ISOC)
- Internet Engineering Task Force (IETF)
- Internet Corporation for Assigned Names and Numbers (ICANN)
- Internet Architecture Board (IAB)

[10] Andrew Harmic, Computer Ethics and Cyber Law http://wikipedia.org/miki/cyberethic accessed 20/9/2015
[11] Ibid

- Council of Registers (CORT)
- Inter NIC.
- International Telecommunication Union (ITU)
- Agency of United Nations that regulates ICT issues (may someday create global standards for policing the Internet.)[12]

The reason for ethical use of information is not the computers but the information stored in the computers. Information ethics are the rules that define right and wrong behavior in the computing profession.

Ethics and laws are not the same. Laws are established to protect software developers (copyright and licensing) and users. Laws have penalties associated with it but ethics do not. Ethics is primarily based on principles and values. Ethics fall into three categories, the professional-which is defined by various professions (For example, lawyers have their own professional conduct or ethics which guide and regulate their activities).

- **Social Ethics:** This is the ethics as defined by the society in which one finds himself. There are certain moral codes or values that are already tailored by the society and the system wants one to fit into them. When one fails to adhere to these moral codes or standards, one will be regarded as social deviant or misfit.
- **Individual Ethics:** This is defined by personal heritage and integral values.

The need for cyber law in Nigeria cannot be over emphasized due to sudden rise of cyber crimes in the country. Recently a report indicated that Nigeria is losing about $80 Million dollars yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research based in South Africa. Also the American National Fraud Information

[12]Andrew Harmic, Computer Ethics and Cyber Law.

Centre reported Nigerian money offers as the fastest online scam, up to 90% in 2001[13]. The centre also ranked Nigeria cyber crime impact per capita as being exceptionally high[14]. Despite the high rate of crime in Nigeria, some scholars are of the view that cyber space should not be regulated while some assert that it should be regulated.

5. Regulation of the Cyberspace.

Cyber space has transformed the way we live in the recent times. It has virtually affected every sphere of the society ranging from the economic, social, educational sector, health sector, military etc. In fact, the cyberspace has transformed the way we communicate, travel, power our homes, run our economy and obtains government services. Cyber law includes rules and regulation that should be applied to curb the menace of cyber crime while ethics involve the application of moral behaviors to control the use of cyberspace. However, some authors aver that the cyber space should not be regulated by proffering the following reasons:

(a) Freedom of Expression should be an Absolute Right

This particular school of taught posits that regulating the Internet will grossly violate the right of privacy of individuals as provided in the*1999 Constitution of the Federal Republic of Nigeria*. Such right is absolute and cannot be qualified without irreparable damage to civil liberty in a free society. However, all rights have to be qualified in order to protect the society because absolute rights threaten other rights. For instance unrestricted right to freedom of expression and the press on the Internet by which pornographic content exist on the Internet would threaten the

[13] Mu'azu A.S. Abubakar M.K Cybercrime in Nigeria: An overview Act 2013, *Journal of Law , Policy and Globalization*
[14] Ibid

right of children to be free from abuses, molestations and embarrassment. Also it is trite that fundamental rights are qualified on the basis of public policy and morality.

(b) The Internet cannot be Regulated Because of its Global Nature

Another argument hinges on the fact that the Internet cannot be regulated because of its complexity. This school of thought asserts that unlike other communication network, the Internet is enormous and is not possible to regulate.

However, this argument is very porous and not tenable because the cyber space remains an electronic data delivery just like other electronic communications networks such as radio, television and other telecommunications. These other networks are regulated and so should the Internet in order to secure the security of the Internet user.

(c) The Internet is Different in Operation from Other Communications.

It is further argued that the cyber space should not be regulated because its use is quite different from other communication network. However, this argument is not tenable because its peculiar operation that requires a particular user, who seeks particular site or application, is the core reason why it should be regulated to avoid disorder or anarchy online.

(d) Parental Control

Another argument is that the Internet should not be regulated by the government or any organization in order to protect children from child abuse which is perpetuated through obscene pornography on the Internet. They assert that children should be protected by their parents and not by the government.

However, it is posited that even though parents, teachers and guardians and supervisors control or limit what children access on the Internet, their effort can still be supported by regulatory authorities.

6. Overview of Legal Framework in Nigeria to Fight Cyber Crime

(a) Cyber Crime Act 2015

In other jurisdiction, such laws that protect cyber users have existed but for Nigeria, it is just starting. The Act is known as the Nigeria Cyber Crimes Act 2015. The new Cyber Crimes Act signed into law on May 15, 2015 stipulates that, any crime or injury on critical national information infrastructure, sale of pre-registered SIM cards, unlawful access to computer system, cyber-terrorism, among others would be punishable under the new law.[15] The objective of the Act is generally provided as follows:-

(i) To provide an effective and unified legal regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes in Nigeria.

(ii) To ensure the protection of critical national information on infrastructure and

(iii) Promote cyber security and the protection of computer system and networks, electronic communication data and computer programs, intellectual property and privacy rights.

Section 2 provides for its application which provides *inter alia* that the provisions of this Act shall apply throughout the Federal Republic of Nigeria. The challenge one faces with this application is the issue of geographical boundary. Knowing that in the cyber space there is nothing like geographical boundary. In fact delinquent youth popularly known as "Yahoo boys" have hidden under this cloak to commit

[15] Joseph Onyekwere, Cyber Crimes Act 2015 and need for further amendment

serious cyber crimes. For instance somebody in Nigeria can commit a crime or dupe a company in America currency that runs in millions of dollars. The absence of international framework and cyber ethics has made the rights to privacy with regards to Internet a mirage.

To make the provision of the law real, efficient and implementable, there should be an international legal framework that will bring the culprit to book whenever on offence is committed in the cyber space.

7. Major Innovations of the Act

The Act has made several innovations to ensure security of Internet users in the cyber space. The major highlights are as follows:

(a) The Act provides for seven years imprisonment for all kinds of computer related fraud, computer related forgery, cyber pornography, cyber –stalking and cyber-squatting.

(b) The Act criminalizes certain acts and omissions, provides best practices and provision of procedural guidelines for the investigation of such offenses.

(c) The Act also defines the liability of service providers and ensures that national interest is not compromised by the use of electronic communication.

(d) To provide a legal framework for the prohibition and punishment of electronic fraud and cyber crime whilst promoting e-government services, electronic communication and transactions between public and private bodies as well as institutions and individuals.

(e) The Act gives the President the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens as

constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furthermore of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.

(f) Prescribes the death penalty for an offence committed against a system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

(g) Hackers, if found guilty, of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

(h) The Act makes provision of identity theft, with the punishment of imprisonment for a term of not less than N7 million or both fine and imprisonment. An example of identity fraud would be the individual who impersonated Chief Bola Tinubu (the former Governor of Lagos State) on Facebook and was apprehended recently by the police.

(i) Specifically creates child pornography offences, with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others, producing, procuring, distributing, and possession of child pornography.

(j) Outlaws Cyber-staling and Cyber-bullying and prescribes punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.

(k) Prohibits cyber squatting which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or fine of not less than N5 million or to both fine and imprisonment.

(l) Forbids the distribution of racist and xenophobic material to the public through a computer system or network (e.g. Facebook and Twitter), it also prohibits the use of threats or violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than N10 million or to both fine and imprisonment.

(m) Mandates that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional right to privacy, and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

(n) Allows for the interception of electronic communication, by way of a court order by a Judge, 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.

The above is just a high-level overview of certain interesting provisions in the newly passed legislation. The Act itself contains 43 sections, and is a very important piece of legislation to foster the development of the nascent ICT sector in Nigeria. Detail of this law can be found in Cybercrime (Prohibition, Prevention) Act

8. Types of Crimes Provided by the Cyber Act

The Cyber Crime Act is made up of 59 section, 8 parts and 2 schedules. The first schedule lists the Cyber Crime Advisory Council; while the second schedule lists businesses to be levied for the purpose of the cyber security fund under **S. 44 (2) (a) GSM** service providers and all telecom companies, Internet service providers; Banks and other financial institutions; insurance companies and Nigeria stock exchange.

The Act provides for various cyber crimes but not limited to the following:

(a) **Cyberstalking:** This includes intentionally sending of mails via computer system that is grossly offensive or pornographic. Also sending false mails to others with intention to annoy, inconvenience, obstruct, insult, cause criminal intimidation to another[16]. It also involves acts that place another person in fear of death violence or bodily harm.[17]

(b) **Cyber Squatting:** This involves intentional use of a name, business name, trade mark, domain name or other word or phrase registered, aimed or in use by any individual, body corporate or belonging to either the Federal, State or Local Government in Nigeria, on the Internet or any other computer network

[16] Cybercrime (prohibition) Prevention Act 2015 sec 24
[17] Ibid

without authority or right and for the purpose of interfering with their use by the owner,[18]

(c) **Manipulation of ATM:** The Act provides that any person who manipulates an ATM machine or point of sale terminal with the intention to defraud shall be guilty of an offence and upon conviction sentenced to five years imprisonments[19]

(d) **Phishing/ Spamming:** The Act provides that any person who intentionally engages in computer phishing shall be liable upon conviction to 3 years imprisonment or a fine.[20]

(e) **Spreading of Computer Virus:** The Act provides that anyone who engages in malicious or deliberate spread of viruses or any malware that causes damage to critical information in public or private or financial institution computers shall be guilty.

These and many more are the various crimes that are protected and provided for by the Act. However, the Act delved into other matters that are not related to the cyber space For instance, financial matters etc.

The principle around cyber crime legislation requires that the law focuses on computer-related offences; content-related offences; computer integrity offences; jurisdiction and procedural issues, international harmonization /relation. But a few of the law indicates that in addition to meeting the foregoing milestone achievement though commendable, the drafters made strenuous efforts in seeking to bank transactions which is not related to the cyber crime.[21]

[18] Ibid sec 25
[19] Ibid sec 30
[20] Ibid sec 32
[21] Ibid

9. Cyber Protection in Nigeria 1999 Constitution

The first point of call for cyber protection under the Nigeria Legal jurisprudence is the *1999 Nigerian Constitution of the Federal Republic of Nigeria*. Section 37 of the Constitution provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.[22] According to the Nigerian Constitution, the individual's right to privacy is sacrosanct. It can only be fettered by laws made by democratically enabled public authorities in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or moral or for the protection of the rights and freedoms of others.[23]

(i) In the interest of defense, public safety, public order, public morality or public health; or

(ii) For the purpose of protecting rights and freedom of other persons" surmising from the above, the right to privacy of an individual even when protected by the Constitution can be compromised by any Act of the federation which seeks to protect public safety, order and interest.

Thus, enforcement of the right of privacy, under the Nigerian constitution may not be readily obtainable; an individual may need to seek redress under other applicable laws.[24]

10. The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act also provide the legal framework for the establishment of the Commission and protection of economic

[22] 1999 Constitution
[23] Ibid
[24] Ibid

and financial crimes. Some of the major responsibilities of the Commission according to part 2 of the Act include:

(a) The investigation of all financial crimes, including advanced fee fraud money laundering, counterfeiting, illegal charge, transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam among others;

(b) The coordination and enforcement of all laws against economic and financial crimes with a view to identifying individual, corporate bodies, or groups involved;

(c) The Act undertakes research and similar work with a view to determining the manifestation, extent, magnitude and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same;

(d) Takes charge of, supervises, controls and coordinates all the responsibilities functions and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes in consultation with the Attorney General of the Federation;

(e) The coordination of all investigating units for existing economic and financial crimes, in Nigeria;

(f) The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1994

(g) The Failed Bank (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended;

(h) The Banks and other financial institution Act 1991, as amended, and miscellaneous offences Act.

According to **section 23 of the Advanced Fee Fraud Act**[25]false pretenses means representation whether deliberate or reckless, made by word, in writing or by conduct of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.

Economic crime is defined by the Act as "the non-violent criminal and illicit activity committed with the objective of earning wealth illegally, either individual or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including countering of currency, theft of intellectual property and policy open market abuse, dumping of toxic wastes and prohibited good.

This is currently the only law in Nigeria that deals with Internet crime issues and it only covers the regulation of Internet service providers and cyber cafés. It does not deal with the broad spectrum of computer misuse and cyber crimes as cited by the Criminal Code.

11. The Nigerian Criminal Code Act 1990

The Criminal Code Act of 1990 criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber crime is not mentioned in the Act, it is a type of stealing punishable under the Criminal Code. The most renowned provision of the Act in **Chapter 38,** deals with obtaining

[25]Advanced Fee Fraud and Related Offences Act 2006 (Source: National Assembly of Nigeria 2006)

property by false pretenses or cheating. The specific provision relating to cyber crime is **section 419,** while **section 418** gave a definition of what constitute an offence under the Act. **Section 418** states that any representation made by words, writing or conduct of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.[26]

Section 419 states that any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. Despite the laudable provisions enumerated in these legal frameworks, cyber crime still thrive in Nigeria because law alone is inadequate to curb the menace of cyber crime. It is therefore recommended that these laws should be combined with ethics to totally eradicate cyber crime in Nigeria.

12. Factors That Exacerbate Cybercrime in Nigeria

(a) **Lack of Jurisdiction:** The problem of jurisdiction has exacerbated the rate of cyber crime in Nigeria. The cyber criminals can sit in the confine of their room and commit a crime that will affect them in other jurisdiction. For instance, he may be in Nigeria and commit an offence that will have effect in South Africa. The question will be which court will have jurisdiction to try the matter, is it the court in Nigeria or the court in South Africa? This challenge has become a stumbling block in arresting the problem of cyber crime in Nigeria.

(b) **Untrained Personnel/Monitoring Team:** Despite the laudable provisions made by the Act, cyber crimes still thrive in Nigeria due to absence of

[26]Maitanmi Olusola, Ogunlere Samson Ayinde Semiu, Adekunle Yinike

trained personnel to prosecute the offenders. Most of the Nigerian police personnel that ought to monitor, arrest and prosecute cyber crime are not computer literate. It is therefore recommended that Nigerian police force should be subjected to constant ICT training to make them grow with the technology and be efficient and effective in their duty.

(c) **Lack of Job:** The poverty rate in Nigeria is very high and has thrown our youths into cyber crime. Some who are graduates do not have a job and in order to survive, they indulge in cyber crime in order to make ends meet. These youths are known as yahoo boys' and are noted for duping people.

(d) **Juveniles Delinquency:** Juveniles are young people that are under the age of eighteen. By virtue of juvenile law they enjoy protection because they are regarded as infants. The truth is that many that engage in cyber crime like phishing, spreading of computer virus, cybersquatting etc are infants that enjoy protection from the law. Thus even when they are caught, the law does not punish but rehabilitate and reintegrate them into the society because they are still malleable.

(e) **Lack of Implementation:** The problem is not the law. The Act has made laudable provision to protect individuals and society from the menace of cyber crimes. The problem lies in implementation. The truth is that as at present, Nigeria does not have viable structures to implement the laws. The prosecutors are not trained; there are no monitoring team to oversee the activities of delinquent youth especially those that operate computer system in cybercafé. Thus lack of implementation cripples the law and makes the right of information technology a mirage to citizens.

(f) **Corruption:** The issue of corruption is the bane of many African countries. For instance the Act provides in Sec 32 (1) that any person who engages in

computer phishing shall be liable upon conviction to three years imprisonment or fine of one million naira.

In Nigeria even when these cyber criminals are caught, the police may demand for bribe which when offered, will close the case. Corruption has enhanced the growth of Internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud. Nigeria was ranked third among the most corrupt countries in the world.

(g) **Lack of Standards and National Central Control:** Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulation standards and computer security and protection act is hampering true e-business. Foreign Direct Investment (FDI) and foreign out sourcing are encouraging computer misuse and abuse[27].

(h) **Lack of National Functional Databases:** National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individuals records and tracing their movements.[28]

(i) **Porous Nature of the Internet:** The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

(j) **Increased Dependency of Computer Systems:** With vulnerability and dependence of computer system within global Internet. The rate of crime and damage of the new Internet technology as a result of criminal activities is significantly increasing.

(k) **Poor Regulation of the Internet.** Cyber crime thrives on weak information protection due to poor regulation of the Internet. It is therefore imperative to

[27] *International Journal of Cognitive Research in Science Engineering and Education* Vol. 1 No1, 2013.
[28] Ibid

give information about vulnerability of computer system due to the Internet use and necessity of effective protection means.

(l) **Complex Cyber Criminal Network:** The emerging trend of criminal organizations working together with criminally minded technology professionals to commit cybercrime as well as fund other activities. These cyber criminal network are inherently complex bringing together individuals in real time from across the globe to commit crime on an unprecedented scale.

(m) **Imperfection of Domestic Legislation and Absence of International Legal Framework:** Imperfection of domestic legislation and absence of International Legal Framework has greatly hiked the rate of cyber crime because great use of the Internet has significantly surpassed current national and international social and legal norm, which regulate the sphere of information protection.

13. Recommendations

(a) **Adequate Legislation and Implementation:** Cyber ethics and cyber laws are being formulated. It is recommended that these laws should be implemented so that the laws will be real. International legislation should be made to avert the problem of jurisdiction which acts as catalyst in exacerbating cyber crime.

(b) **Training/Continuous Education:** Citizens and stakeholders should be trained on the use of the Internet to be abreast with the latest trend in the cyber space in order to maneuver the schemes of cyber criminals. The police and other law enforcement agencies should undergo continuous education for effective security management.

(c) **Creation of Information Technology Awareness:** Information Technology forums should be created to enhance the lives of the Nigerian youths so that they will not be trapped into cyber crimes.

(d) **Interactive Voice Response (IVR) Terminal:** Technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer.[29].

(e) **Cryptography:** Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient[30].

To totally arrest the menace of cyber crime in Nigeria, it is imperative that outdated and obnoxious laws be totally overhauled to bring them *interdem* with current social and legal norm. Apart from imperfection of domestic laws, there are no precise definition and classification of cyber crime, coupled with the difficulty of interpretation and application of the regulating law enforcement agencies activities in this respect. The necessary mechanism of ensuring activities and cooperation of the law enforcement agencies for regulation of the Internet as well as proper detection and punishment of cybercrimes is not yet well developed.

14.Conclusion

The recent increase in cyber crime is a major concern to the world especially with regards to e-commerce. This ugly trend has affected virtually all sectors of the society and is negatively affecting the image of the country. Nigeria is rated as one of the countries with the highest level of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country negatively to the

[29]Ibikunle Frank, Eweniyi Odunayo, *Approach to cyber security issues in Nigeria: challenges and solution*.
[30]Ibid

outside world. It is therefore imperative that a combination of sound technical measures, laws and ethics are used to counter the activities of cyber criminals. Fighting cyber crime requires a holistic approach to combat this menace in all ramifications. The government, stakeholders and every member of the society should exercise duty of care towards other Internet users. That is ethics, and international legal framework should be put in place to regulate the Internet; laws that cannot effectively regulate the cyber world should be jettisoned. There is also need for the government, security agencies to note that there is need to keep up with technological and security advancement.

References

1. Ademola Samuel Adeniyi, The Need For Data Protection Law In Nigeria. https://adeadeniyi.wordpress.com.2012/07/18,the-need-for-data-
2. Alfreda Dudley,James Braman, Giovanni Vincent, *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices USA*, 2011.
3. Andrew Harmic, *Computer Ethics and Cyber* Law http://wikipedia.org/miki/cyberethic
4. Cyber Crime (Prohibition) Prevention Act 2015.
5. Freedom of Information Act 2011.
6. Ibikunle, .F, Eweniyi .O, Approach to Cyber Security Issues in Nigeria: Challenges and Solutions, *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE).*
7. Joseph Onyekwere,Cyber Crimes Act 2015 and need for further amendments.The Guardian Newspaper, 24 August, 2015.
8. Kashmir Musa Waziri, The Legal Regime of Parents and Designs Law and its Effects on National Development. *International Journal of Humanities* vol.3, No. 2, 2011

9. Leah McGrath Goodman,How Washington opened the floodgates to online poker dealing parents a bad hand.http://www.newsweek.com

10. Nigerian Law Intellectual property Watch (NLIP) https://blips.com/some-basic-facts about-patent-in- Nigeria

11. Ufuoma Barbara Akpotaire,Patent Strategies for companies Doing Business in Nigeria.http://ssrn.com/abstract=1801883.