An Assessment of the Impact of Municipal Laws on the Policing of Cyber Crimes in Nigeria

Dr. Rasul 'Yomi Olukolu

Lecturer & Sub Dean, Department of Jurisprudence & International Law, Faculty of Law, University of Lagos, Lagos, Nigeria

Abstract

Internet crime can be defined as unlawful acts using the computer as either a tool or a target or both. Internet networks are used positively to conduct businesses, manage industrial and governmental activities, engage in personal communications and conduct researches. Also certain confidential information are stored or passed through the medium of the internet. Credit cards containing information of users are used as the major means of buying and selling on the internet. Information infrastructure has become a critical part of the backbone of global economies, therefore, it is imperative that the general public be able to rely on the availability of such informational services with confidence that their communications and data are safe from unauthorized access or modification. It then becomes important for these and other information to be more secured. However, the speed of the internet, its affordability and its elimination of distance make the internet the hotbed of crimes globally. Cyber crime growth has skyrocketed in recent times especially in Nigeria, hence the need for immediate action by law makers to stem the tide. This research, therefore, examines the adequacy or otherwise of the Nigerian legal framework in checking crimes being perpetrated using the internet as a platform with a view to making useful suggestions.

Keywords:

I. Introduction

I. Introduction

The revolution in information technology and telecommunication has brought with it benefits and advantages for development and the improvement of the quality of life. It has facilitated the exchange of ideals, dissemination of information and improved service delivery especially in developed countries where necessary associated infrastructure is widely available. But this is one side of the story . The same revolution has also brought in its wake new methods of criminality with mind-boggling impact and precision.

The gap that the digital revolution bridged has facilitated not only improvement in service delivery with the other benefits of the revolution but also provides the fertile ground for crime and criminality of highest ingenuity that cannot be easily tracked of traced except by or with equally sophisticated technology and understanding. Associated with this challenge is the legal regime under which such crime and criminality may be dealt with since in most cases the criminality has extra territorial effect requiring new laws with which to prosecute.

However, the global information society is evolving at a neck break speed where accelerating convergence between telecommunications, multimedia and information and communications technology (ICT) drives new products and services as well as ways of conducting business and

[51]Bolaji Owasanoye (Prof) "Computer Crime Detection and Prosecution", (unpublished) p.1.

[52]Ibid, p.1

commerce. This has been made possible by the opportunities offered by the internet. Information networks are used to conduct business, manage industrial and governmental activities, and engage in personal communications and conduct research.

The world is transiting to a competitive, dynamic and knowledge based economy and in the words of Nicholas Negroponte "the change from atoms to bits to unstoppable." Information infrastructure has become a critical part of the backbone of global economies, therefore it is imperative that the general public be able to rely on the availability of informational services and they should have confidence that their communications and data are safe from unauthorized access or modification.

Certain confidential information are stored or passed through the medium of the internet, credit cards containing information of users are used as the major means of buying and selling on the internet. It then becomes important for these and other information to be more secured.

The speed of the internet, its affordability and its elimination of distance make the internet the hotbed of crimes globally. Cyber crime growth has skyrocketed in recent times, hence the need for immediate action by law makers to stem the tide.

The purpose of this research is, therefore, to examine the adequacy or otherwise of the Nigerian legal framework in checking crimes being perpetrated using the internet as a platform and to proffer useful suggestions.

II. History of the Internet

The internet was the result of some visionary thinking by people in the early 1960's that saw great potential value in allowing computers to share information on research and development in scientific and military fields.

J.C.R Licklider of Massachusetts Institute of Technology (MIT) first proposed a global network of computers in 1962 and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to develop it. Leonard Kleinrock of MIT developed the theory of packet switching which was to form the basis of internet connections. Lawrence Roberts of MIT connected a Massachusetts computer with a California computer in 1965 over dial up telephone lines. It showed the feasibility of Wide Area Network but also showed that the telephone lines circuit switching was inadequate.

The internet then known as ARPANET was brought online in 1969 under a contract led by the renamed Advanced Projects Agency (ARPA) that initially connected four major computers at universities in the Southern United of America.

The internet was designed in part to provide a communication network that would work even though some of the sites were destroyed by nuclear attack. It was brought about as an effect of the United States arm race with the Soviet Union which began in 1957 with the launch of Sputnik 1 that is man's first artificial satellite.

Further breakthrough which followed the first international connection was made in 1973 from ARPANET to the University of London as well as the 1980 development of "Because it's lime network" (BITNET) which connected IBM mainframes around the educational community and the world to provide cheap mail services beginning in 1981.

---

[53]"Being Digital", New York, 1995 at www.tokypc.org/newsletter/1995/07/bedigit.html (visited on 25 June 2017).

[54]www.walthowe.com/navnet/history.html (visited on 26 June 2017).

Subsequently, the number of hosts began to increase dramatically reaching 10,000 in 1987 and breaking 100,000 in 1989, despite ARPANET being formally decommissioned in 1990 . The internet continued to grow in leaps and bounds with prestigious institutions like the National Library of Medicine going on line. But it was perhaps in 1991 that the web emerged with two major events taking place. The National Science Foundation (NSFNET) lifted the commercial restriction on the use of network, thus opening a means for electronic commerce. All pretences of limitations on commercial use disappeared in May 1995 when the NSI; ended the sponsorship of the internet backbone and traffic relied on commercial networks, AOL prodigy and CompuServe came online.

Internet Language defined FOREVER with EER, the European Organization for Nuclear Research, the World largest particle physics laboratory popularly known as CBRN'S release of the World Wide Web and the creation of the Hyper Text Markup Language (HTML) that uses Uniform Resources Locators (URL) for web address by Tim Berners-Lee. From then on history ran its course with impunity. The internet momentum was unstoppable with everyone from the World Bank to the White House going on line.

Finally the Mosaic and the research engine GOOGLE have transformed the unknown frontiers of yesterday into what are now playgrounds for the present. The cyber community is now as real as ifs physical counterpart. In Nigeria, Licenses for internet connections were first granted to internet service providers (ISP) in 1995 by the Nigerian Communication Commission. These ISP companies then in turn connect willing hosts to the web in exchange for sums of money. Other trend on the development of the Web is the growth of other devices to the internet such as laptops, small tablets, pockets computers, smart phones etc.

III. The Darkside of Cyberspace

The internet has indeed served to empower individuals and organizations with information sharing, dissemination, research and development. However, this power is available not only for progressive purposes but also for destructive and criminal purposes. Whilst the internet has facilitated enormous ease and growth of business, it has also been used for the ease and growth of criminal activities.

It has been reported that since 1993, attacks on the computer systems of bank and other financial institutions made possible by the use of the latest generation of military weapons which target communication systems have resulted in loss of about 500 million pounds as the organisations involved paid ransom money . According to the Federal Bureau of Investigation figures, United State of America, company's losses due to internet fraud in 2003 surpassed US $500 million.

In recent years, there have been prosecutions for the possessions and publications of child pornography both in the United Kingdom and the United States, this being material that was available either on computer networks or on other electronic media. Such examples serve to illustrate how the computer can be used to assist the perpetration of crime.

---

[55]Parang Diwan etal (ed); Fundamentals of Information Technology, (Vol. 1), Pentagon Press, New Delhi, 2005, p. 10.

[56]See www.walthowe.com/navnet/history.html (visited on 28 June 2017)

[57]See http://cern.ch/CERN/.Geneva/Switzerland (visited on 30 June 2017)

[58]Diane Rowland & Elizabeth Macdonald; Information Technology Law, 2nd edition, Cavendish Publishing, London, (1996) p.22.

[59]See http://en.wiki/internet-fraud (last visited on 2 July 2017).

Although computer hacking is what comes to mind when computer abuse and misuse is referred to, there is a wide spectrum of activity that may be referred to as internet crimes that began to become apparent as the so called computer or information revolution progressed.

Thus, August Baquai, writing in the preface to an early Council of Europe Recommendation on Computer-related Crimes suggests that,

"In the information society, power and wealth are increasingly becoming synonymous with control over our data banks… the computer revolution has provided tools with which to steal with impunity, to control and manipulate thought and movement of millions and hold on entire society hostage."

Thus, the dangers of cyberspace have been spelt out more recently by Ulrich Sieber in his report to the European Commission presented in January 1998 entitled "The legal aspects of computer related crime in the information society", in his words:

"The vulnerability of today's information society in view of computer crime is still not sufficiently realized, businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. In the businesses community, for example, most of the monetary transactions are administered by computers in the form of deposit money. Electronics commerce depends on safe systems for money transactions in computer networks."

A company's entire production frequently depends on the functioning of its data processing system. Many businesses stored their most valuable company secrets electronically. Marine, air and space control systems as well as medical supervision rely to a great extent on modern computer systems.

Computers and the internet also play an increasing role in the education and leisure of the international minors. The international computer networks are the nerves of the economy, the public sector and the society. The security of these computers and communication systems and their protection against computer crime is therefore of essential importance.

In the course of the development, computer crimes have developed into major threat of today's information society. The spreading of computer technology into almost all areas of life as well as the interconnection of computers by international computer networks has made computer crimes more diverse, more dangerous and internationally present.

According to the then Chairman of the Nigerian Economics and Financial Crimes Commission (EFCC), Mallam Nuhu Ribadu , about $6 billion has been lost between 1989 and 1996 to internet fraud globally. According to an American survey , 85% of companies which experience a major breakdown in their computer systems as a result of crackers go out of business within eighteen months.

Bringing it home, the EFCC boss stated that Nigerians have defrauded people using the internet to the tune of about $700 million between May 2004 and June 2010 and that there are currently 500 suspects and about 100 cases being handled at the courts. He further stated that internet crimes are the fastest growing brand of crimes in Nigeria. These problems are very appalling in Nigeria. According to Wasik

---

[60]See Council of Europe Recommendation on Computer Related Crime, 1990, p.4.

[61]See the Report for the European Commission of the Outcome of the COM CRIME Study available at www.ispo ccc.bc/legal/en/criine.html (last visited on 2 July, 2017).

"the sheer diversity within the context of computer misuse, where the computer may figure at one moment as the instrument of crime and as the target for crime and given the importance of non economic notices in some forms of computer systems purely for intellectual challenge and some cases of computer sabotage, makes any monolithic exploration of this phenomenon quite implausible "

IV. Defining Internet Crime

Internet crime has been defined as follows: "It encompasses any criminal act dealing with computers and networks (called hacking)…" A broad attempt was made in the Telecommunications and Postal Offences Act, No. 21 of 1995 to define an 'internet crime' to mean:

"Any person who inter alia engages in computer fraud or does anything relating to fake payments whether or not the payment is credited to the account of an operator or the account of a subscriber is guilty of an offence."

Professor Owasanoye defines 'internet crime' as any crime committed by a person using a computer as the vehicle or the means to the nefarious end. The whole notion of computer crime ought not to be odious to the imagination considering that the emergence of telecommunication technology brought with it novel crimes. For example, in Nigeria, it was possible for unauthorised calls to be made and the bill passed unto an unsuspecting subscriber. Until recently, this was a trademark of the inefficient and grossly corrupts national telephone company, the Nigerian Telecommunications Limited (NITEL).

In spite of these experiences, there is a school of thought that feels that the notion of computer crime is a myth because many of the crimes are simply age-old schemes or offences committed over a medium. While it must be accepted that computers themselves do not commit crimes, it cannot be denied that the persons who use them do. However, those who feel that any criminal activity involving a computer is computer crime are also right because without the medium of the computer, perhaps, the crime would not have been committed.

The commission of the offence in question is never in doubt; the problem is the proof of its commission because most of the steps are electronic in nature. Electronic records such as computer networks, logs, e-mails, word processing files will invariably provide the prosecution with important evidence in criminal cases. But how does the prosecution analyse, understand and present electronic evidence stored in computers?

Internet crimes are perpetrated in about three ways. With Computer being the target of crime, its confidentiality, integrity, or availability is attacked. Computer could also be a tool used to commit crimes. In this category, the computer is not essential for the crime to occur but it is related

---

[62]Nuhu Ribadu; "Problems Associated with Enforcement of EFCC Laws Against Economic Crimes", a Paper presented at the Nigerian Bar Association Annual Conference, Abuja, 23 – 27 August, 2004, p. 10.

[63]Reported on "Computing Magazine", October 22, 1992, p. 27. See also New Law Journal, Vol. No. 6596, p. 540.

[64]See http://www.messagingpipeline.com(last visited on 4 July 2017)

[65]Nuhu Ribadu, supra note 12.

[66]M. Wasik; Crime and the Computer, Clarendon Press, Oxford, 1990, p. 83.

[67]www.webopedia.com (last visited on 2 August 2017)

[68]Section 2 A (h).

[69]Bolaji Owasanoye; "A Legal Perspective to Economic Crimes and Fraud", a Paper presented at the Round Table on The Role of Forensic Investigative Accounting: Challenges for the Banking Industry, 19th July, 2010, Nigerian Institute of Advanced Legal Studies, Lagos.

to the criminal act. Lastly, a computer is used to store evidence and even though the computer is not directly used for criminal purposes but the evidence can be of great value to criminal investigations.

V. Categories of Internet Related Criminal Activity

This range of financial and economic criminal activity in Nigeria covers a wide range of internet crimes. Some of these will now be espoused below.

a. Credit Card Fraud

One of the fastest- growing categories of Internet fraud is payment card (i.e. credit card and debit card) fraud. Online credit card fraud causes substantial problems for online merchants. Initially, many online merchants were defrauded when people, using others credit card numbers, ordered merchandise and had it shipped to foreign locations that were clearly different from the addresses of the true credit card holders. To commit online payment- card fraud, criminals need access to valid payment-card numbers. One means of acquiring them is the unlawful accessing of e-commerce websites. For example, in the case of United States v. Bosanac , the defendant was involved in a computer hacking scheme that used home computers for electronic access to several of the largest United States telephone systems and for downloading thousands of calling card numbers. The defendant, who pleaded guilty to possession of unauthorized access devices and computer fraud, used his personal computer to access a telephone system computer and to download and transfer thousands of access codes relating to company calling card numbers. The defendant was sentenced to eighteen months imprisonment and $10,000 in restitution.

b. False Merchant Website

In this situation, the criminal is running a merchant website usually adult site which accepts credit cards for access as proof of age. In all of these cases, the consumer's actual account is never changed. Once the identities are gathered the suspect makes purchase on real merchant sites, or acquires cash advances on the accounts. In Nigeria, the Economic and Financial Crime Commission (Establishment) Act No 5 2004 is charged with the responsibility of investigating and processing of all Economic and Financial crimes. Perhaps, the closest offence is found in section 1(1) of the Nigerian Advanced Fee Fraud and other Related Offences (Amendment) Act of 2006 which provides

"Notwithstanding anything contained in any other enactment or law, any person who by any false pretence and intent to defraud (a) obtains from any other person in Nigeria or in any other country for himself or any other person: or (b) induces any other person, in Nigeria or in any other country to deliver to any person, any property, whether or not the property is obtained or its delivery is through the medium of a contract induced by false pretence commits an offence under this Act."

c. Identity Theft

A cyber criminal can either take over someone else's credit card account or steal his identity to create a new credit account; these accounts are then used to attack e-businesses.

---

[70]J.K Robinson, Assistant Attorney General, Criminal Division, United States of America in a paper on the "Internet as the Scene of Crime" at the International Computer Crime Conference, Oslo, Norway (May 29, 2000) at www.usdoj.gov (last visited on 10 July 2017).

[71]S.D. Cal filed December 7, 1999 (unreported).

In essence, the suspect completes an order form using the false information; the web merchants accept the order and then ship the goods and services to the suspect. One key difference from the traditional in-store fraud is that the criminal can hit the derailed merchants and do a lot of damage very fast in the virtual world of the internet. The suspect does not have to drive between shops or does not have to speak to a telephone operator to commit their crime.

Some Nigerians abroad are reputed to open credit card accounts online with someone else's identity. They would run up thousands of dollars in charge within days using the stolen identity when they are through. They dispose of the credit card and return to Nigeria with the stolen money. This explains why imported goods cost less than the manufacturer's price and this trend is sometimes erroneously believed to be money laundering fronts.

The instant credit accounts issued on the internet are completed and set up in a few minutes given the speed with which instant credit is approved. It is not surprising that fraudsters will continue to prey on the willingness of the bank or merchant to issue an instant account. These entities understand the potential risk and will quickly write-off losses when faced with a non paying customer. The information needed to create new accounts can be gathered from a variety of sources including trash bins, legitimate files or even public records.

d. The Nigerian 419 Scam

A worldwide scam which has run since the early eighties is the Advanced Fee Fraud also known as 419 frauds. It is named after the relevant section of the Criminal Code of Nigeria.

The scam operates as follows: the target receives an unsolicited fax, email, or letter often concerning Nigeria or other African nation containing either a money laundering or other illegal proposal or one may receive a legal and legitimate business proposal by normal means.

Common variations on the scam include over invoiced or double invoiced oil or other supply and service contracts where the culprits want to get the average out of Nigeria. It also involves ordering items and commodities off trading sites on the web and then cheating the seller. The variations of Advanced Fee Fraud (419) are manifold and they are virtually endless.

At some point, the victim is asked to pay up front an advanced fee. The Advanced Fee Fraud and other Fraud Related Offences Act, 2006 was enacted to showcase the presence of these crimes in Nigeria and the Economic and Financial Crimes Commission is now charged with the responsibility to enforce this Act.

e. Cyber Pornography

This would include pornographic websites including transmission of images to children, pornographic magazines produced using computers and the internet to download and transmit pornographic pictures, photos, writings e.t.c. The disseminations of pornographic via the internet have raised numerous legal questions. The major issues that need to be examined are in respect of the liability of the author of the material and the additional liability of the network provider.

[72]Economic and Financial Crimes Commission Act, 2004. This Act was enacted to ease the proof of these crimes and the Economic and Financial Crimes Commission is now charged with the responsibility of enforcing this Act.

[73]Section 17, Advanced Fee Fraud and other Fraud Related Offences Act, 2006.

[74]For example, see the Penal Code (Northern States) Federal provisions Act, laws of Nigeria, 2004; the Obscene Publication Act 1961; and the Criminal Code Act, Laws of Nigeria, 2004.

[75]Sunday 20, July 2003.

Under the Nigerian law, an obscene publication includes sending of a publication albeit (obscene) by post.

f. Internet Husbands

A story was featured in The Observer (UK) about one Anastasia Solovieva, a citizen of the former Soviet Union signed up with a mail order bride agency. The agency matched her with a fat, bald man in Seattle (USA) more than twice her age; she left Russia to marry the man in America.

The attractive 18 year old was determined to make her US marriage work. In some early letters home to her parents in Kyrgyzstan, she praised her husband for his intelligence and smart dress sense.

Two years after their wedding, Anastasia was dead, strangled and buried in a junkyard by her husband. Anastasia had no idea that her husband was a violent thug divorced from a first overseas bride who testified in court of how he had been beaten her regularly and pounded her head against a wall.

The mail order bride industry is booming with abuses. Some States in America plan to introduce legislation to offer greater protection for 4000 - 6000 women mainly from former Soviet bloc countries and the Philippines, who came to the United States each year for marriage.

This crime is not common in Nigeria for the reason that there is the inability of the mail order bride agency to secure visas for the girls here and the attendant financial constraints.

g. Online Sale of Illegal or Stolen Articles

Prohibited goods, including illegal drugs, are reportedly being marketed and sold on the internet at one time or the other. One of the most common types of internet crime is online auction fraud. The vendor may be describing the products or services in a false or misleading manner or may take orders and money but failed to deliver the goods or the seller may supply counterfeit goods instead of legitimate ones or even stolen goods.

Under the Nigerian Firearms Act , it is an offence to own or sell a firearm without having the required license. The problem is how can one determine the culpability of a transaction on the internet involving unlicensed foreign seller and a buyer, for instance.

h. Online Gambling

Many websites today offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Gambling is not an offence under Nigerian laws. However, in order to ascertain when gambling is a front for money laundering, it is required that casinos should keep records of gamblers who visit them under the Nigerian Money Laundering (Prohibition) Act .

The question posed here is whether the same responsibility can be imposed on an ISP hosting an online casino originating from Nigeria. Online gambling in law involves the creation of risk

---

[76]Laws of Nigeria, 2004.

[77]Money Laundering (Prohibition) Act, 2011.

[78]D. Baumer & L. Poindexter; Cyber Crime and E-Commerce, McGraw Hill Companies, New York, 2001, p. 38.

[79]Criminal Code Act, Laws of Nigeria, 2004.

[80]Laws of Nigeria, 2004.

that has no prior existence whereas speculation, hedging and other risky ventures essentially involve transferring of risk from one party to another rather than creation of risk .

i. Intellectual Property Crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code . A situation may arise whereby a Nigerian illegally downloads music software or book from the internet. How can the owner seek redress?

In Nigeria, computer programs are protected by the Copyright Act . Traditional penal provisions easily cover theft of corporeal information (e.g. books, papers, CD ROMS, Floppy disks).

j. Cyber Defamation

This occurs when defamation takes place with the help of computers and the internet. For instance, someone publishes defamatory matter about someone else on website or send mails containing defamatory information to that person's friends. This offence is traditional in nature. For example 'defamation' is defined in Section 142 of the Sharia Penal Code Law of Zamfara State of Nigeria as 'spoken or reproduced words by mechanical means intending to harm or knowing or having reason to believe that the reputation of the person will be harmed'.

k. Web Jacking

This occurs when someone forcefully takes control of a website by hacking the password and later changing it. The actual website owner does not have any more control over what appears on that network.

In Nigeria, this type of internet crime is common through hacking of notable persons' websites and with a view to swindling unsuspecting members of the public. It is also common in Nigeria to have employment websites of companies and corporations being hacked with a view to seeking from unsuspecting members of the public non-existing job offers in such companies and corporations.

l. Stock Market Manipulation Scheme

They are also called investment schemes online. Criminals use these to try to manipulate securities' prices on the market for their personal profit. According to the United States' Securities and Exchange Commission, the two methods used by these criminal are

i. Pump and Dump schemes: where false or fraudulent information is disseminated in chart rooms, internet boards, and via emails with the purpose of causing dramatic price increase in traded stocks or stocks of shell companies. As soon as the price reaches a certain level, criminals immediately sell out their holdings of those stocks realising substantial profits before the stock price falls back to its usual low level; and

ii. Short Selling or Scalping schemes: this is similar to the pump and dump scheme in terms of approach. They disseminate false or fraudulent information through chart rooms and forums e.t.c. with the purpose of causing dramatic price decreases in a specific company's stock. Once the stock reaches a certain low level, criminals buy the stock and then reverse the false information or just wait for it to wear off with time. Once the stock goes back to its normal level, the criminal sells the stock and reap the huge gain.

m. Cyber Terrorism

The final category of cyber crimes is the newest and most dangerous threatening not only the present but also the future, the cyber terrorism. The criminals usually have a lot of power behind them (in the form of organised crime against hostile foreign or national governments) to commit great damages and will usually not stop at anything less than the physical or economic destruction of their targets. Their drive is not necessarily financial but may also be a specific cause they defend. Cyber terrorists have dominated the global scene in terms of the most devastating and harmful crimes committed on the internet in the world today.

VI. Impact of Internet Crimes in Nigeria

Nigeria, a nation of about 160 million people, is reputed to be one of the countries with high presence of internet crimes and a leader in the scamming industry. According to a World Bank study, a quarter of urban college graduates are unemployed, crime therefore offers tempting career opportunities in drug dealing, illegal immigrant, trafficking and most of all internet fraud.

According to the then EFCC Chairman, Mallam Ribadu, cash and assets worth more than $700 million has been lost between May 2003 and June 2004 to online fraud committed by Nigerians.

Reuters, an American press organisation in 2001 stated that 48% of global email is spam out of which 6% is Nigerian email. In a report by the American National Fraud Information Centre, Nigerian money offers 4% of total internet fraud.

It was also recently reported that Nigerians scammers attempted to get money through the United States' hurricane Katrina disaster by launching a fake website to collect donations.

The British Broadcasting Corporation once described Nigeria as a hotspot for scamming. In the same vein, Reuters reported in 2000 that "Campaigners say it (419) is now the third to fifth largest foreign exchange earner in Africa's most populous nation"

Thus, to the international community, as a result of the activities of these scammers, the generality of Nigerians are portrayed as fraudulent and corrupt people. Furthermore, the combined impact of these crimes is the restriction of business dealings between Nigerian companies and their foreign counterparts among other things. Private companies around the world are also taking steps to block email traffic originating from Nigeria. Recently it was reported that the biggest domain registrar in the world "Go daddy software Inc" and owners of the web domain www.godaddy.com, where individuals can buy packages of web domains and resell to other individuals has blocked Nigerian's internet protocol address because, according to it "Nigeria was identified as a country where there was a high incidence of fraud".

The impacts of these crimes include the portrayal of Nigeria as a dangerous and business unfriendly atmosphere. The impact of this is to scare away potential investors from investing in Nigeria. Cyber crimes also have negative impact on the nation's security where hackers have

---

[82]See http:www.nigerianvillagesquare1.com/articles.oyesanya.html (last visited on 12 July 2017).

[83]Nuhu Ribadu, supra note 12.

[84]See http://www.fraud.org/2002 instats.htm (last visited on 12 July 2017).

[85]See http/www.messagingpipeline.com(last visited on 4 July 2017).

[86]See http//www.messagingpipeline.com/(last visited on 4 July 2017).

[87]Omotola Awe; "Cyber Fraud Leads to Blockage of Nigeria's IP Address," Punch Newspapers of January 4, 2006.

consistently targeted the websites of some of the top government organisations like the Central Bank of Nigeria.

The seeming ease and success of some of these cyber criminals also have the impact of portraying cyber fraud as an alternative to gaining employment. This attitude is gradually growing especially among the youths and it portrays great danger for the future. There is, therefore, the need on the part of the government to do more in terms of fortifying the existing laws on internet crimes and the creation of employment and enabling environment for businesses to thrive in Nigeria.

VII. The Nigerian Law and Internet Crimes

The quarter century between 1945 and 1970 can be seen as the first stage in the evolution between law and computers. There are many issues to be resolved in cyber law. For instance in Nigeria, there is the dearth of judicial authorities on cyber law and there are no major statutory schemes. Policy makers and attorneys dealing with cyber crimes are often confined to referring to the imprecisely applicable and scarcely existing statutes and cases.

It is submitted, however, that the existing Nigerian legal framework on internet/cyber crimes is insufficient and there is the need to upgrade the existing ones in line with what obtains in the international comity of nations.

In Nigeria, most legislations dealing with the conventional crimes now perpetrated using the internet were enacted without the possible criminal online scenario in mind. Thus most of the statutes do not make for online provisions. However, It is submitted that as a stop gap and pre-step to a necessary and inevitable legislative upgrading, the existing criminal law and legislations could be given wider interpretation to cater for online cases. A critical analysis will now be made of the current state of legislation in tackling internet/cyber crimes in Nigeria.

i. Advanced Fee Fraud and Other Fraud Related Offences Act, 2006

This Act provides that:

(1) "Notwithstanding anything contained in any other enactment or law, any person who by false pretence and with intent to defraud- (a) obtains from any other person in Nigeria or in any other country for himself or any other person; or (b) induces any other person, in Nigeria, or in any other country, to deliver to any person, or (c)obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act. (2) A person who by false pretence and with intent to defraud, induces any other person in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act."

This provision, although, does not specifically capture on line transactions where the identity of the person to be defrauded is not ascertainable, it is submitted that the Nigerian courts should as a matter of necessity interpret the foregoing provisions to ensure the conviction of an accused person, whenever, the provisions call for interpretation.

---

[88]Stewart Biegel; "The Emerging and Specialised Law of the Digital Revolution", , Daily Journal, Los Angeles, January 25, 1996, p.1.

[89]See the United States' Computer Fraud and Abuse Act, 1986 as amended. The US model was made to respond fully to changes in technological development in the areas of computer –generated evidence, privacy, searches, seizures of computer generated evidence. See also the South African Electronic Communications and Transactions Act, 2002 which represents a genuine one-stop national e-strategy legislation to facilitate e-commerce and combat computer crimes and information system abuses.

ii. Criminal Code Act, Laws of Nigeria, 2004

With regards to an offence like identity theft where a cyber criminal can take over somebody else's credit and account or steal his identity to create a new credit account, the criminal code could be interpreted to deal with the crime. The closest definition to the above described offence is provided for in section 419A of the Criminal Code Act which states:

"Any person who by any false pretence or by means of any other fraud obtains credit for himself or any other person incurring any debt or liability; or by any means of an entry in a debtor and creditor account between the person giving and the person receiving credit is guilty of a felony..."

The question here is "how do you apply the traditional provisions of obtaining credit by false pretence to the unauthorised "appropriation" of electronic information? The offence of theft or stealing requires that tangible property be taken away with the intention of permanently depriving the victim of same. Applying the traditional concepts to acts involving intangible information can only mean that amendments to our criminal statutes are inevitable.

Occurrences on the internet where people give false credit card details in order to access a merchant store to perpetuate fraud can give rise to some interpretation difficulties. For a fraud to be deemed to have occurred, it is necessary that a "person must be deceived", where the machine is the one deceived to obtain a service, no person as such is deceived.

A further complication is that, although an apt offence may be identified, the nature of computer technology may make it more difficult to identify both when and where the offence occurred, both of which factors may have important ramifications for the final outcome of the case.

The potential difficulties that may arise in such situations are illustrated by the facts of Thompson's case, an English authority. Thompson was a computer programmer employed by a bank in Kuwait. He identified five accounts that were both made into or out of them for a long time. He then opened five accounts in his name at various branches of the bank and transferred money into these accounts from the dormant accounts. He travelled to the United Kingdom and opened accounts in UK banks and further wrote to the Kuwait Bank manager asking him to transfer the money now in five accounts held in his own name. This led to him being suspected. He was charged and convicted. The Law Society in England recognising this lacuna suggested that the definition in the Theft Act, 1968 should be extended by introduction of the wordings: "inducing a machine to respond to false representations which the person making them knows to be false as if they were true."

The above proposal, however, was not acted upon and it remains the position that "The prevailing opinion is that it is not possible in law to deceive a machine"

With regards to the Advance Fee fraud ('419' scam), the Criminal Code Act provides 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."

---

[90]Laws of Nigeria, 2004.

[91](1984) 1 Weekly Law Report 962.

[92]Diane Rowland and Elizabeth Macdonald,supra note 8, p. 453.

[93]J.C. Smith; Law of Theft, (8th Ed.), Butterworth, London, 1997, p. 97.

It is, however, still not clear whether software stolen, or password hacked will constitute intangibles as to be capable of being stolen under the Nigerian law.

iii. Endangers Species (Control of International Trade and Traffic) Act, Laws of Nigeria, 2004

With regards to online sale of animal species threatened with extinction, this Act should be upgraded to tackle online sales. Problems may arise where the sale is carried out across two countries and two different legal systems. The implications of this are that an upgrade or review of this law must be done with the jurisdictional issues involved borne in mind.

iv. Cyber Defamation Law

The Criminal Code Act, Laws of Nigeria, 2004 criminalises defamation generally. Defamation can also, generally, be treated in the realm of civil law of tort in Nigeria. 'Defamation' was defined by the Nigerian Court of Appeal in Nigeria Television Authority v. Ebenezer Babatope as

"... a statement which is published of and concerning a person and calculated to lower him in the estimation of right thinking person or cause him to be shunned or avoided, to expose him to hatred, contempt or ridicule... "

Cyber defamation is one of the very few species of cyber crimes which is adequately catered for under the traditional provisions of the Criminal Code Act under section 374.

Thus, a defamatory material sent as an email or meant to be published on the internet can be interpreted and construed under section 374(2) which states: "... causing it to be read or seen... "

v. Evidence Act, Laws of Nigeria, 2004

In all the aforementioned cases, while the legislation on the subject may be upgraded, certain aspects may still pose some problems, for instance, the means of proving by evidence in all cases may remain difficult as the Nigerian law of evidence does not seem to contemplate electronic evidence. A review of the Nigerian law of evidence principally the Evidence Act shows that several changes must be made in the law, to ensure the accommodation of digital and electronic data in the applicable rules of evidence. The Nigerian law of evidence as presently constituted is inadequate to deal with online crimes.

Ancillary matters which require review are covered in other sections of the Act. For instance, the option of expanding the provisions of section 74(1) which addresses evidence of "judicial notice" should be interpreted to include electronic and digital materials should be considered as an interim measure.

Other areas include rules relating to admissibility of evidence: standards of proof of evidence, signature certification of documents etc. are areas requiring review. While section 121 of the Evidence Act addresses admissibility of evidence, with respect to telegraphic messages, judges /magistrates appear to be left to conjure applicable presumption with regards to digital and electronic data. It then becomes clear that an unambiguous definition of 'information and

[94]Laws of Nigeria, 2004.

[95]Section 374.

[96](1996) 1 Nigerian Weekly Law Report (Part 440), 75.

[97]Laws of Nigeria, 2004.

communication technologies' (ICTs) in the Evidence Act is a critical necessity at this stage of our legal development.

In Nabu v. NAL Merchant Bank the Nigerian Court of Appeal rejected admissibility and evidential relevance of computer generated bank account statements. This judicial reasoning failed to take account of the more than a decade of commercial banking trend in Nigeria. An amendment of the Evidence Act will resolve this and other evidential issues affecting electronic communications.

vi. Criminal Procedure Act and Police Act, Laws of Nigeria, 2004 - Police Power of Arrest

It is pertinent to note that under Section 10 (1) (f) of the Nigerian Criminal Procedure Act, the Police may arrest and detain any person who might have committed fraud on the internet outside Nigeria provided such act constitutes an offence under the law of the country where the act was done. The Act empowers the Police to apprehend and detain such a person in Nigeria.

Section 28(1) of the Police Act should, however, be amended to allow for seizure with or without warrant. Accordingly, in pursuance of the Police powers to investigate and prosecute crimes under the Nigerian Police Act, computers and other electronic gadgets and equipment containing digital data and electronic information should be within the powers of the Police to seize whenever there is a reasonable suspicion that such had been used to perpetrate crimes.

vii. Nigerian Consumer Protection Council Act, 1992

The Consumer Protection Council Act establishes the Consumer Protection Council. It provides for the protection of the interests of consumers in relation to purchase and consumption of goods and services that are purchased on offline basis. There is no specific provision in the Act for goods and services procured online. Thus, there is the need to amend section 2 of the Act to include internet based procurement of goods and services and empower the Council to make appropriate regulations for the general protection of consumers in cyberspace on the other hand with a view to reducing or stemming online sale of illegal and stolen goods, credit card frauds and false merchant syndrome amongst other internet crimes which affect consumers generally.

viii. Conclusion

Computer information which is the main object of computer crime is characterised by extreme mobility which exceeds by far the mobility of persons, goods, or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds. This mobility of computer data in international computer networks makes international solutions for fighting computer crime indispensable.

Combating cyber crime involves not only the deployment of men and materials but also application of ethical and legal values. There is the need not to forget to educate the public especially the youth that computer crimes are as lethal and dangerous and illegal as the traditional known crimes.

---

[98]Federation Weekly Law Report (Part 145), 661at 666.

[99]Laws of Nigeria, 2004.

[100]1992, No 68.

Different national strategies with the aim of preventing computer crimes would create computer crime havens which in turn would lead to market restrictions and national barriers to the international and worldwide services. In the United States, the Department of Justice is working with the private sector in an effort to forming the cybercitizen partnership, an initiative designed to educate and raise awareness of computer responsibility. Nigeria should borrow from this.

However, the growing danger from crimes committed against computers or against information on computers is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are unlikely to be enforceable against such crimes. This lack of legal protection means that businesses and government must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

In a nutshell, for a national information technology policy to be effective, it must be carried out in cooperation with international bodies and other foreign countries. Moreover, national solutions and restrictions for the free flow of information will be doomed to failure since the amount of data transferred in international computer networks makes controls of their contents neither possible nor socially desirable.

Above all, Nigeria must enact new laws or radically upgrade the existing ones to fight computer related crimes. A comprehensive and thorough review of existing criminal statutes and other legislations with regards to online criminal offences as stated makes this suggestion inevitable. With regards to Nigeria, there is need for a basic legal response to computer related conduct just as we have in developed countries.

References

1. Nicholas Negroponte; *Being Digital*,1995, Alfred A. Knopf, New York.
2. M. Wasik; *Crime and the Computer*, 1990, Clarendon Press, Oxford.
3. Diane Rowland and Elizabeth; *Information Technology Law*, 1997, Cavendish Publishing Limited, UK.
4. ParangDiwan,R.KSuriand, Sanjay Kaushik, *Fundamentals of Information Technology*, Vol. 1, 2005, Pentagon Press, New Delhi.
5. I.T Encyciopaedia.com 2nd revised Edition, vol.9. Pentagon Press, New Delhi, 2005.
6. J. C. Smith; *Law of Theft*, 8th Edition, 1997, Butterworths, London, 1997.
7. D. Baumer& L. Poindexter; *Cyber Crime and E-Commerce*, 2001, McGraw Hill Companies, New York.
8. Stewart Biegel; "The Emerging and Specialisd Law of the Digital Revolution", *Daily Journal*, Los Angeles, January 25, 1961.
9. BolajiOwasanoye; "A Legal Perspective to Economic Crimes and Fraud", a Paper presented at the Round Table on The Role of Forensic Investigative Accounting: Challenges for the Banking Industry, 19th July, 2010, Nigerian Institute of Advanced Legal Studies, Lagos.
10. J.K Robinson, Assistant Attorney General, Criminal Division, United States of America in a paper on the "Internet as the Scene of Crime" at the International Computer Crime Conference, Oslo, Norway (May 29, 2000) at www.usdoj.gov (last visited on 10 July 2017).
11. Economic and Financial Crimes Commission Act, 2004, Laws of Federation of Nigeria (LFN), 2004.
12. Nigeria's Advanced Fee Fraud and Other Related Offences Act, 2006.
13. Criminal Code Act, LFN, 2004.

[101]See www.witsa.org (last visited on 15 September 2017).

[102]See for example England Computer Misuse Act of 1990; and the United States' model.

14. Penal Code (Northern States) Federal Provisions Act, 2006.
15. Obscene Publication Act, 1961.
16. Criminal Procedure Act, LFN, 2004.
17. Police Act, LFN, 2004.
18. Money Laundering (Prohibition) Act, 2011.
19. Copyright Act, LFN, 2004.
20. UK's Computer Misuse Act, 1990.
21. United States' Computer Fraud and Abuse Act, 1986.
22. South Africa's Electronic Communications and Transactions Act, 2002.