CURTAILING CYBERCRIME IN NIGERIA: APPLICABLE LAWS AND DERIVABLE SOURCES

Abstract
The innovation in computer, information communication infrastructure and internet, cuts across every human endeavour in Nigeria. It has also created avenue for miscreants to engage in cybercriminality against cyber citizens. Since the economic gains emanating from the use of the computer, internet and other digital paraphernalia to perpetrate cybercrime by cybercriminals outweigh the consequences of their act, in the event they are caught, they are likely to continue in their illegality. This is further exacerbated by the anonymity of the internet; lucrative nature and awareness of the subject area; greed and potential targets increment; the fact that it requires smaller investment to start and that it can be carried out in various locations without any iota of geographical constraints. The proliferation of cybercrimes in Nigeria has generated debates in the literature as to whether or not there exists legal framework for effective and efficient investigation and prosecution of cybercrimes in Nigeria. In this regard, this paper examines the literature and consequently, enlist applicable laws and derivable sources that will generally be handy to stakeholders; law enforcement agents; prosecutors; counsel to eradicate cybercrime in Nigeria.

Keywords: Cybercrime, Cybercrime Law, Applicable Laws in Nigeria, Derivable Sources, Impact of Cybercrime

1. Introduction
The global perpetration of cybercrime through the internet is no longer a hidden phenomenon. It has raised serious concerns for all a sundry. The characteristics of the internet have made the internet very popular. The reliance of the internet and computers within the last few years has revolutionized the way and manner things are carried out in Nigeria. The medium of communication within and outside the country is now very easy. The prevalence of information on the internet for the benefit of Nigerians and as a source for information is another added advantage. Nigerians patronize e-mail, blackberry messenger, yahoo messenger and even text messages in legal training and practice, negotiations, settlement discussions, confidential communications, transaction closings and the completion of contracts for goods and services. In short, the impact of the internet and computers to the lives of Nigerians, both personally and professionally, cannot be overemphasized.

\*Felix E. EBOIBI, Ph.D(Law), LL.M(Nig.), LL.B(Cal.), BL(Nigerian Law School), Lecturer, Faculty of Law, Niger Delta University, Wilberforce Island, Nigeria. E-mails: felixeboibi@mail.ndu.edu.ng or lixboibi@yahoo.com; Tel:+2348033175431
1 M.M. Kamal, et.al., ‘Nature of Cybercrime and Its impact on Young People: A Case from Bangladesh’ (2012) 8(15) Asian Social Science, 1
Irrespective of these notable additions to Nigerians, drawn from the availability of the internet and computers, criminal elements have taken advantage of these resources to further their criminal acts. It is a specie of e-related crime referred to as cybercrime, where a computer is either used as a tool or target or it involves elements of information technology infrastructure. Cybercrime has become so dangerous and notorious in Nigeria. The crime has resulted to a lot of havoc to corporate organizations, cyber citizens, governments within and outside Nigeria. Its attributes amongst others are seen in: adverse reduction of competitive strength of corporate organizations; unnecessary time wasting and sluggish economic/financial growth; delays production and increases cost; tarnishes Nigeria image; facilitates the growth of terrorists’ activities; it has impact on consumer trust; it enhances money laundering; it encourages fraud on social media; it is a danger to our national security.

Against this backdrop, bulk of the literature tilts towards assertions nicknaming Nigeria as the hub of cybercrime and cybercrime perpetration and how it has embarrassed Nigeria and damaged her international reputation. Generally, the assertions are hinged on the unavailability of cybercrime


3 Ibid
laws in Nigeria to facilitate the investigation and prosecution of cybercrime perpetrators. For instance, a commentator⁶ had argued before now about the damaging nature of cybercrime in Nigeria and alluded to the fact that Nigeria is a place where computer can be used to commit all sorts of crimes without prosecution, as there is no law on cybercrime.⁷ Another commentator⁸ recognizes the growth of cybercrime perpetuation in Nigeria and attributed same to the lack of internet specific laws.⁹ On the other hand, a commentator, rightly, offered quite a number of possible Nigerian legislations, though unexhaustive, within the reach of law enforcement agents in Nigeria to prosecute cybercrime perpetrators.¹⁰

In order to effectively curtail cybercrimes in Nigeria, comprehensive cybercrime legislations ought to be put in place to guide against the commission of these crimes and negate the tolerance of same. Moreover, when they take place, perpetrators should be convicted for the crimes, adequately effective in order to dissuade them and others. These ordinarily, require well defined cybercrime legislations for the prosecution of cybercriminals.¹¹ Has the Nigerian legal system clearly captured legislations for the prosecution of cybercriminals? Are there applicable laws and/or derivable sources of law in the Nigerian polity to curtail the menace of cybercrime?

In this vein, this paper generally examines mandatory regulations regulating cyber citizens in Nigeria, premised on legal reasoning in an attempt to fill the gap in the literature of the absence and/or unexhaustive applicable laws to try cybercriminals. Without delineations, it takes a general look at primary and secondary legislations and applicable case laws that contain judicial precedent. These may be national, international or regional.

---

⁸ Ibid
⁹ Ibid
2. Cybercrime Eradication: Search for Applicable Laws and Derivable Sources.

An examination of the applicable laws available for the investigation and prosecution of cybercriminals in Nigeria would be incomplete without first of all determining what cybercrime law entails. The existence of a cybercrime law in a nation cannot be overemphasized. It is a veritable tool in the hands of law enforcement agents to curtail online activities. In this respect, lawmakers have the primary authority to equip them with a cybercrime law to carry out their functions.

One thing that is paramount in a cybercrime law is its provisions in respect to cybercrime litigation. It provides express liability and strict or stringent remedies against perpetrators of cybercrime. This is particularly important because electronic/internet abuses are getting out of control. Cyber citizens are consequently exposed to computer/online fraud, identity theft, harassment etc. Intellectual property invasions against corporate organizations and tertiary institutions are in the increase or perpetrated by cybercriminals. Top government secrets are being attacked and hijacked by foreign authorities.\(^{12}\)

The possible lawful measure to provide solution in respect to these unwanted cyber activities is by imposing liability. Cyber citizens should be availed legal means to seek redress for the protection of their properties, rights to information technology and intellectual paraphernalia.\(^{13}\) Quite obvious and germane is a cybercrime law that gives law enforcement agents efficient and effective legal tools for investigating and curtailing electronic invasions and unlawful conducts. In this category also is an avenue for prompt and effective prosecution of perpetrators. It should contain provisions relating to the nature and scope of liability, increased sentences and forfeiture powers; protection for cybercitizens or ordinary internet users. A cybercrime law is a valuable and effective tool for combating cybercrimes.\(^{14}\)

Based on the foregoing, Cybercrime Law or Law and Cybercrime denote legal issues or framework that relates to the use of computers, communications technology and the internet. In essence, it is an attempt to apply laws designed for human activity on cyberspace and to regulate cyber citizens. In Nigeria, a law that aims at making comprehensive provisions on all aspects of cybercrime is the Cybercrimes (Prevention, Prohibition Etc) Act 2015. Moreover, there are other Nigerian prevailing laws that are in use for the investigation and prosecution of cybercrime perpetrators: Constitution of the Federal Republic of Nigeria, 1999 (as amended); Economic and Financial Crimes Commission (Establishment) (EFCC) Act 2004; Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, 2006; Money Laundering (Prohibition) (Amendment) Act, 2012; Nigerian Communications Act 2003; Evidence Act 2011; National Information Technology Development Agency(NITDA) Act 2007.

These laws are discussed hereunder seriatim, while also examining their relationships with cybercrime.


\(^{13}\) Ibid.

\(^{14}\) Ibid.
2.1 Cybercrimes (Prevention, Prohibition Etc) Act 2015

The Nigerian Cybercrimes (Prohibition, Prevention, etc) Act 2015 is the first Nigerian cybercrime legal and regulatory framework enacted to regulate the activities of persons in the cyberspace and cybercrimes in Nigeria. The explanatory memorandum and objective of the Act encapsulates the true and express intendment of the Act, demonstrating the deterrence theory of punishment. The Act is punitive in nature and this is as a result of the prevailing and escalating menace of cybercrimes in Nigeria. It provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution and punishment of cybercrimes and other related matters. Precisely, the Act offers an avenue for cybersecurity and consequently, fortifies the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights as well as preservation and protection of the critical national information. The Act in her Section 1 contains the objectives of the Act which are invariably similar to the explanatory memorandum of the Act. The Act provides in Section 2 that “the provisions of this Act shall apply throughout the Federal Republic of Nigeria.” This implies that none of the 36 States House of Assembly can lawfully and rightly enact any law regulating cybercrime in a State. The doctrine of covering the field contained in Section 4(5) of the Constitution of the Federal Republic of Nigeria (as amended) 1999 seem to have been amplified by this provision. It states that where a law enacted by the House of Assembly of a State is inconsistent with any law validly made by the National Assembly, the law made by the National Assembly shall prevail.

The Act is apportioned into 59 Sections; 8 parts; and 2 Schedules. Part I of the Act contains the object and application of the Act and encompasses Sections 1 and 2 of the Act. Part II of the Act deals with the protection of critical national information infrastructure and comprises Sections 3 and 4 of the Act. Part III covers offences and penalties, which includes; - Offences against critical national information infrastructure; Unlawful access to a computer; System Interference; Interception of Electronic messages, e-mails, electronic money transfer; Tampering with critical infrastructure; Willful misdirection of electronic messages; Unlawful interceptions; Computer

---

16 Cybercrimes (Prohibition, Prevention, etc) Act 2015, explanatory memorandum.
17 Ibid., s. 1.
18 Constitution of the Federal Republic of Nigeria (as amended) 1999, s.4 (5).
19 Cybercrimes (Prohibition, Prevention, etc) Act, 2015, s.5.
20 Ibid., s.6.
21 Ibid., s.8.
22 Ibid., s.9.
23 Ibid., s.10.
24 Ibid., s.11.
25 Ibid., s.12.
related forgery;\textsuperscript{26} Computer related fraud;\textsuperscript{27} Theft of electronic devices;\textsuperscript{28} Unauthorised modification of computer systems, network data and system interference;\textsuperscript{29} Cyber-terrorism;\textsuperscript{30} Fraudulent issuance of e-instructions;\textsuperscript{31} Identity theft and impersonation;\textsuperscript{32} Child pornography and related offences;\textsuperscript{33} Cyberstalking;\textsuperscript{34} Cybersquatting;\textsuperscript{35} Racists and xenophobic offences;\textsuperscript{36} Importation and fabrication of e-tools;\textsuperscript{37} Breach of confidence by service providers;\textsuperscript{38} Manipulation of ATM/POS terminals;\textsuperscript{39} Phishing, spamming, spreading of computer virus;\textsuperscript{40} Dealing in card of another;\textsuperscript{41} Purchase or sale of card of another;\textsuperscript{42} Use of fraudulent device or attached e-mails and websites\textsuperscript{43} and incorporates Sections 5 to 36 of the Act. Part IV embodies the duties of financial institutions/duties of service providers and contains Sections 37 to 40 of the Act. Part V deals with administration and enforcement and embodies Sections 41 to 44 of the Act. Part VI incorporates arrest, search, seizure and protection and comprises Sections 45 to 49 of the Act. Part VII embraces jurisdiction and international co-operation and contains Sections 50 to 56 of the Act. Part VIII provides for miscellaneous issues of regulations, interpretation and citation and contains Sections 57 to 59 of the Act. The first schedule of the Act lists the members of the Cybercrime Advisory Council while the Second schedule lists businesses to be levied for the purpose of the Cybersecurity Fund under Section 44(2) (a) of the Act.

\textbf{2.2 Constitution of the Federal Republic of Nigeria, 1999 (as amended)}

The Constitution of the Federal Republic of Nigeria, 1999 (as amended) has useful provisions regarding a privacy right which is against cybercrime; illegal computer hacking or online stalking etc. by private or official persons. The Constitution of the Federal republic of Nigeria, 1999(as amended) equips Nigerians with the right to privacy, homes correspondence, telephone conversations and telegraphic communications.\textsuperscript{44} Consequently, where there is the need for law enforcement authorities or security agencies to request for information contained in individual’s

\textsuperscript{26} Ibid., s.13
\textsuperscript{27} Ibid., s.14.
\textsuperscript{28} Ibid., s.15.
\textsuperscript{29} Ibid., s.16
\textsuperscript{30} Ibid., s.18.
\textsuperscript{31} Ibid., s.20
\textsuperscript{32} Ibid., s.22
\textsuperscript{33} Ibid., s.23
\textsuperscript{34} Ibid., s.24.
\textsuperscript{35} Ibid., s.25.
\textsuperscript{36} Ibid., s.26.
\textsuperscript{37} Ibid., s.28.
\textsuperscript{38} Ibid., s.29.
\textsuperscript{39} Ibid., s.30.
\textsuperscript{40} Ibid., s.32.
\textsuperscript{41} Ibid., s.34.
\textsuperscript{42} Ibid., s.35
\textsuperscript{43} Ibid., s.36
\textsuperscript{44} Constitution of the Federal Republic of Nigeria, 1999(as amended), s.37.
mobile phones, e-mails etc in course of investigation through service providers in respect to cybercrime perpetrated, due regard must be had to individual’s right to privacy under the Nigerian Constitution. Moreover, the Nigerian Cybercrimes Act 2015 and its provisions must not be read and enforced in isolation. The Constitution is more or less a check on the enforcement of the provisions therein; hence caution must be taken in respect to the observance of human rights and internet freedom in Nigeria. Despite section 45(1) (b) of the Constitution in this regard, the Supreme Court through one of its most respected jurists, Justice Kayode Esho in Rasome Kuti v Attorney General of the Federation stated thus: “Fundamental Right is a right which stands above the ordinary laws of the land and which in fact is antecedent to the political society itself. It is a primary condition to a civilized existence…”

The implication of the above is that the Nigerian Constitution protects citizens from searches and seizures that are unreasonably carried out by law enforcement agencies. It implores law enforcement agents to obtain a warrant before searching an area where an individual has a reasonable expectation of privacy. The Constitution is the foundation for the protection of standalone computers and the data or information on individual computer from searches by law enforcement agents. Individuals possess privacy in respect to their personal computers, though this right only relates to property he or she owns, possesses or controls. A search warrant must contain and describe the place to be searched and the items to be seized with particularity. This requirement will ensure that the search is limited to suspected criminal activity because cases of computer searches can turn into sweeping examinations of a wide array of information given the wide variety of information stored on almost any computer network. Exceptions must therefore not be granted to the express procedure outlined in sections 39 and 45 of the Cybercrimes Act 2015.

2.3 Economic and Financial Crimes Commission (Establishment) (EFCC) Act 2004

The Economic and Financial Crimes Commission (EFCC) Act 2002 established the Economic and Financial Crimes Commission (EFCC) to halt all economic and financial related crimes in Nigeria. The Economic and Financial Crimes Commission (EFCC) Act 2002 was repealed and enacted to be the Economic and Financial Crime Commission (Establishment) Act 2004. Since the EFCC was established, it has been mandated by its establishment Act with special powers to investigate any person, corporate body, or organization who has committed any Act relating to Economic and Financial Crimes. Section 7 (2) of the EFCC Commission (Establishment) Act 2004, equipped the Commission with the responsibility of enforcing the provision of:

a) The Money Laundering Act 2004; 2003 No. 7 1995 No. 13(as amended)
b) The Advance Fee Fraud and Other Related Offences Act 2006
c) The Failed Banks (Recovery of debts) and Financial Malpractices in Banks Act 1994, as amended.
d) The Banks and Other Financial Institution Act 1991, as amended
e) Miscellaneous offences Act
f) Any other law or regulations relating to economic and financial crimes including the criminal code or penal code.

46 EFCC (Establishment) Act S. 7
It is safe to say that the EFCC (Establishment) Act 2004, empowers the EFCC to investigate and prosecute perpetrators of cybercrimes (Internet or online advance fee fraud in Nigeria) while placing reliance on the Advance Fee Fraud and other related offences Act 2006. For instance in Harrison Odiawa vs Federal Republic of Nigeria,\textsuperscript{47} the accused person who impersonated to be Abu Belgore was arraigned by the EFCC on 58 Count of offences; Conspiracy to obtain by false pretence, obtaining by false pretence, forgery, uttering and possession of documents containing false pretence contrary to the Advanced Fee Fraud and Other Related Offences Act. In course of the trial, the prosecution testified that a solicitation e-mail was sent to one Mr. George Robert Blick (the nominal complainant), an American citizen resident in Virginia, USA by the accused and his cohorts seeking a foreign contractor to facilitate the transfer of $20.5 million US dollar, in the said mail he was asked to respond if he was interested and Mr. George did by e-mail stating that he had a United States registered corporation that could be used to receive the said funds. For the purposes of documentation and finalization of the contract, the accused and his cohorts demanded for several sums of money from the accused through exchange of e-mails, telephone conversations and fax ranging from 187,000 US dollars (creation of new documents), 10,000 pounds (opening of bank account), 18,750 US dollars (trust processing fee), 410,000 US dollars (payment for issuance of ICP number), 750,000 US dollars (resolution of petition against the transaction), 250,000 US dollars (for Nigerian Minister of Finance before ICP number can be issued), 350,000 US dollars (for newly appointed Nigerian Minister of Finance), 300,000 Euros (for transportation), 1.5million US dollars (for the repair of damaged part of machine), 1.2million dollars (for insurance of machine), which Mr. George obliged them. Thereafter, communications between the parties ceased and then it was done on Mr. George that he had been defrauded. He consequently wrote a petition to the EFCC which led to the arrest of the accused. At the conclusion of hearing, Hon. Justice J.O.K. Oyewole held that “from the evidence adduced by the prosecution, it is evident that the accused and his cohorts had a common intention to defraud Mr. George and acting in concert they did obtain the various sum of money contained in counts 2, 8, 10, 12, 14, 18, 20, 22, 24 and 28 from him and found the accused guilty as charged thereon having proved her case beyond reasonable doubt.”\textsuperscript{48} Dissatisfied with the judgment of the court, the accused appealed to the Court of Appeal. The Court of Appeal dismissed the appeal and affirmed the judgment and conviction and sentences of the trial court.

2.4 Advance Fee Fraud and Other Fraud Related Offences (AFF) Act, 2006
Another source of Law and Cybercrime is the Advance Fee Fraud and Other Related Offences Act 2006. This Act replaced the Advance Fee Fraud and Other Related Offences Decree No. 13 of 1995.


\footnote{48} The accused was also found guilty of the offences of conspiracy, forgery, uttering and in possession of documents containing false pretences.
The Act punishes “advance fee fraud”\(^{49}\) (419).\(^{50}\) The Act prohibits, amongst others, ways to combat cybercrime and other related online frauds. These acts prohibited under the Act includes: obtaining property by false pretence,\(^{51}\) use of premises for fraudulent activities,\(^{52}\) fraudulent invitation,\(^{53}\) laundering of funds obtained through unlawful activity,\(^{54}\) attempts,\(^{55}\) conspiracy, aiding and abetting.\(^{56}\) The Nigerian Supreme Court have had course to entertain an online Advance Fee Fraud case; \textit{Mike Amadi vs Federal Republic of Nigeria}\(^{57}\) where the Appellant(Mike Amadi) was charged before the High Court of Lagos State holden at Ikeja by EFCC \textit{inter alia} with attempt to obtain the sum of US$125,000.00 (One Hundred and Twenty Five Thousand United States Dollars) from one Fabian Fajans by sending fake e-mails through his mail box princemike2001@yahoo.com, registered websites efccnigeria.com, Reddiff.com. India Limited, multilink telephone number 017946846 in respect to a forged Central Bank of Nigeria payment schedule containing false pretence by requesting for money to process the transfer of Two Million, Five Hundred Thousand United State Dollars ($2.5 million USD) being the contract sum for the generators Fabio Fajans was purported to have supplied the Federal Government of Nigeria for the All African Games 2003 and by falsely representing to Fabio Fajans that the said sum of US$125,000.00 represent the five percent(5) processing fees of the total sum of USD 2.5 million contrary to sections 5(1), 8(b) and 1(3) of the Advance Fee Fraud and Other Related Offences Act Cap. A6 Vol. 1, Laws of the Federation of Nigeria 2004 now 2006. On 20 May 2005 the High Court found him guilty and sentenced him to 16 years imprisonment. Aggrieved with the judgment of the High Court, the Appellant appealed to the Court of Appeal. The Court of Appeal affirmed the judgment of the High Court. On further appeal to the Supreme Court, the Supreme Court while dismissing the appellant’s appeal, the judgment and sentences of the High Court and the Court of Appeal were affirmed.

Moreover, the Act also made certain provisions by imposing duties on electronic communications service providers such as telecommunications service providers, Internet service providers and owners of telephone and Internet cafes for the purpose of intercepting or halting the use of the Internet and telecommunications facilities in the perpetration of advance fee scams. For instance, the Act obliges any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form to obtain full names; residential address, in the case of an individual; corporate address, in the case of corporate bodies) from customer or

\(^{49}\) The concept “advance fee fraud” implies all fraudulent activities perpetrated with the intent of obtaining money from another person by false pretence. On the other hand, by virtue of section 20 of the AFF Act 2006, False Pretence refers to “a 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”

\(^{50}\) 419 originates from section 419 of the Nigerian Criminal Code Act, cap.77 Laws of the Federation of Nigeria, 1990 and it is the first Nigerian criminal statute to punish the act of obtaining money by false pretence.

\(^{51}\) Nigerian Advance Fee Fraud and Other Related Offences Act, 2006, s.s 1 & 2.

\(^{52}\) Ibid., s.3.

\(^{53}\) Ibid., s.4.

\(^{54}\) Ibid., s.7.

\(^{55}\) Ibid., s.s. 5 & 6.

\(^{56}\) Ibid., s.8.

\(^{57}\) (2008) 12 SC (pt.III) 55 or 36.2 NSCQR 1127
subscriber. It is an offence for a subscriber/customer or service provider not to comply with the identifying information requirement.

The Act also foist it upon any person or entity who engages in the business of providing telecommunications or internet services or the owner or person in the management of any premises being used as a telephone or internet café or by whatever name called to register with the Economic and Financial Crimes Commission; to maintain a register of all fixed line customers which shall be liable for inspection by any authorized officer of the EFCC and also submit returns to the EFCC on demand on the use of its facilities. In *Nnachi Ephraim vs Federal Republic of Nigeria*, the Appellant was convicted at the Federal High Court Kaduna pursuant to the charges of operating Prime Gate Cyber café at No. 1 Abakiliki, carrying out Internet and Telecommunications services contrary to the provisions of section 13(1) (a) and punishable under section 13(5)(c) of the Advance Fee Fraud and Other Related Offences Act 2006 by the EFCC. Aggrieved by the judgment of the Federal High Court, the Appellant appealed before the Court of Appeal Kaduna. The Court of Appeal, while setting aside the conviction and sentence of the Appellant held per Orji-Abadua, J.C.A on the offence of non-registration of cybercafé – (When a person can be said to have committed an offence under section 13(1)(a) of the Advance Fee Fraud and Other Related Offences Act 2006) as follows:

For a person to be guilty under section 13(1)(a), the person must in the normal course of business, provide telecommunications or internet services, or must be the owner or the person in the management of any premises being used as a telephone or Internet café or whatever name called. I must observe that the fact that the signboard of primegate cybercafé is posted at No. 1 Okpara Street, Abakiliki notwithstanding, there must be some over act on the part of the owner of the cybercafé to prove that he actually provides telecommunications or internet services to the public. There was no shred of evidence adduced by the prosecution establishing that Primegate Cybercafe was indeed providing telecommunications and Internet services at No. 1 Okpara Street Abakiliki. The fact that the signboard of Primegate is hanging thereat does not constitute any proof that the said cybercafé was providing any internet services at the said address. I think the saying; ‘the hood does not make the monk’ suits appropriately here. All the documents tendered before the lower court profoundly showed that it was Artifice Colony cybercafé that was indeed providing both the telecommunication and internet services at No. 1 Okpara Street, Abakiliki and not Primegate. P.W.1 admitted that no investigation was

---

58 Nigerian Advance Fee Fraud and Other Related Offences Act, 2006, s.12(1)
59 Ibid., s.12(2) – the section states that “any customer or subscriber who (a) fails to furnish, the information specified in subsection (1) of this section; or (b) with the intent to deceive, supplies false information or conceals or disguises the information required under this section, commits an offence and is liable on conviction to imprisonment for a term of not less three years or a fine of N100,00.; s.12(3) in addition to the above penalty makes service providers to forfeit the equipment or facility used in providing the service.
60 Ibid., s.13(1)(a) & (b). The essence of the compulsory registration with the EFCC is to facilitate the documentation of record of businesses engaged in the provision of telecommunications
61 (2012) LPELR – 22363(CA)
carried out by the EFCC to decipher whether Primegate cybercafé was indeed taken over by Artifice Colony cybercafé or not. They did not obtain the tickets and receipts normally issued to customers to strongly establish that it was Primegate cybercafé that was running the said business. The question is; ‘If there was no proof that Primegate was indeed offering any internet or telecommunication services, where then lies the offence?’ It is only when the cybercafé or a person is offering the services enumerated in section 13(1)(a) of the Advance Fee Fraud and Other Related Offences Act 2006 that the person or the entity is required in law to register the same. A moribund or defunct company, whose signboard is still hanging out on its former business address without any iota of proof of it running any business thereat, cannot be said to be carrying out the same services it had wound up, merely because of the continued display or affixation of its signboard at its former business address. It is not an offence to carry out such internet or telecommunication services or being the owner or person in the management of any premises being used as a telephone or internet café without registration of the cybercafé. There must be proof of the usage of the place as a telephone or internet café. This was lacking in the evidence proffered by the prosecution in the instant case. It is glaring that the judgment of the lower Court was not properly guided in line with principles of law. The Court terribly erred. Accordingly, I find the decision of the lower Court as being perverse.  

Furthermore, anyone whose normal course of business involves the provision of a non-fixed line or Global System of Mobile Communication (GSM), or is in the management of any such services is mandated to submit on demand to the EFCC any data or information necessary or expedient for giving effect to the enforcement of the AFF Act by the EFCC.  

By virtue of section 13(3) of the Act, telecommunications and service providers owe a duty of care to ensure that their services and facilities are not utilized for unlawful activities. However, Orji has questioned the absence of definition of “duty of care” by the Act. He opined that it could be said to mean the report of any suspicious activity by service providers that has to do with the use of its facilities for the perpetration of an advance fee fraud; that a service provider for the purpose of halting criminal actors from using its facilities to commit an advance fee fraud, appropriate measures should be taken; that it may also mean the possibility of holding electronic communications service providers liable should they fail to implement technological measures to prevent online advance fee fraud. He gave instances of failure of implementation of technical measures to prevent the use of its facilities for sending spam e-mails consisting of advance fee fraud proposals.  

Failure on the part of electronic communications service providers to comply with the aforementioned duties expressly provided for in section 13(1) and (2) of the Act commits an offence and is liable on conviction to imprisonment for a term of not less than three years without an option

---

62 Ibid., at pages 44-46.
63 Nigerian Advance Fee Fraud and Other Related Offences Act, 2006, s.13 (2).
of fine and in the case of a continuing offence, a fine of ₦50,000 for each day the offence persists. In a situation where any person or entity has been convicted more than once under the Act, such an electronic communications service provider’s operational license shall be revoked or cancelled. It must be noted that it is a valid defence for any provider of wire or electronic communication service, its officers, employees or agents or other specified persons for providing information or facilities to the EFCC in any cause, matter or suit that the said provider, its officers, employees or agents or any other specified persons acted in compliance with the obligations imposed under the Act.

2.5 Money Laundering (Prohibition) (Amendment) Act, 2012
Cybercriminals amass money through their illegal activities, but find it difficult to spend same on luxury goods they desire. To enable them acquire these luxury goods, their criminal proceeds would have to be transformed for it to appear legal, which is money laundering. Traditionally most monies laundered through the financial system are done in the big financial centers around the world. Basically, money laundering occurs in three steps. First, cash is introduced into the financial system by some means (placement), the second involves carrying out complex financial transactions in order to camouflage the illegal source (layering) and the final step involves acquiring wealth generated from the transactions of the illicit funds (integration). The practice goes on unabated in the banking industry despite existing regulations, possibly because some of the launders have controlling interest in banks and more importantly the fees earned from such phoney transactions boost banks’ income and invariably the balance sheet. Some launderers buy controlling shares in weak banks, while cash-intensive business gives out generous commission to banks on such transactions and as such banks do not scrutinize such proceeds. Even when they fail to comply, the regulatory institutions have been known to turn a blind eye to non-compliance. Consequently, to curtail the above anomaly, the Money Laundering Act 2004 was enacted and subsequently repealed by the Money Laundering (Prohibition) Act 2011. Recently, the Money Laundering (Prohibition) Act 2011 was amended by the Money Laundering (Prohibition) (Amendment) Act 2012 to expand the scope of Money Laundering offences and enhance customer due diligence measures.

The Act makes provision for the prohibition of the laundering of proceeds of crime or illegal act. Though, cybercrime is not expressly mentioned in the Act, proceeds of cybercrime perpetrated by cybercriminals would appear covered by section 15 of the Money Laundering (Prohibition) (Amendment) Act 2012. The section states:

15(1) Money laundering is prohibited in Nigeria. (2) Any person or body corporate, in or outside Nigeria, who directly or indirectly (a) conceals or disguises the origin of; (b) converts or transfers; (c) removes from the jurisdiction;

65 Nigerian Advance Fee Fraud and Other Related Offences Act, 2006, s.13 (5).
66 Ibid., s.13(4).
68 Ibid.
69 Ibid.
70 Ibid.
71 Ibid.
or (d) acquires, uses, retains or takes possession or control of; any fund or property, knowingly or reasonably ought to have known that such fund or property is, or forms part of the proceed of an unlawful act; commits an offence of money laundering under this Act.\footnote{Money Laundering (Prohibition) (Amendment) Act 2012, s.15 (1) & (2). Emphasis is mine.}

The unlawful act referred to in section 15(2) of the Act above includes by virtue of section 15(6) of the Act:

- Participation in an organized criminal group, racketeering, terrorism, terrorist financing, trafficking in persons, smuggling of migrants, sexual exploitation, sexual exploitation of children, illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking, illicit trafficking in stolen goods, corruption, bribery, fraud, currency counterfeiting, counterfeiting and piracy of products, environmental crimes, murder, grievous bodily injury, kidnapping, hostage taking, robbery or theft, smuggling (including in relation to customs and excise duties and taxes), tax crimes (related to direct taxes and indirect taxes), tax crimes (related to direct taxes and indirect taxes) extortion, forgery, piracy, insider trading and market manipulation or any other criminal act.\footnote{Ibid., s.15(6). Emphasis is mine.}

Cybercrime having been outlawed by the Cybercrimes (Prohibition, Prevention Etc) Act 2015, it therefore means that perpetrators of same may invariably engage in an organized group to perpetuate incidence of cybercrimes; fraud; forgery covered under section 15(6) above. Cybercrime can be interpreted to come under “any other criminal act” used therein. Consequently, proceeds from acts perpetrated by cybercriminals are unlawful and when they are laundered, they are held to have committed the offence of money laundering. Anyone who violates section 15(2) of the Act\footnote{Money Laundering (Prohibition) (Amendment) Act 2012, s.15 (3).} is liable on conviction to a term of not less than 7 years but not more than 14 years imprisonment\footnote{Ibid., s.15(4).} but where it is a body corporate, liability is on conviction to- (a) a fine of not less than 100% of the funds and properties acquired as a result of the offence committed; and (b) withdrawal of licence.\footnote{Ibid., s.15(5).}

Where the body corporate persists in the commission of the offence for which it was convicted in the first instance, the Regulators may withdraw or revoke the certificate or licence of the body corporate.\footnote{Nigerian Communications Act, 2003, s.1.}

\section*{2.6 Nigerian Communications Act 2003}

The Nigerian Communications Act was put in place in 2003 with the primary aim of creating and providing a regulatory framework for the Nigerian Telecom or Communication Industry.\footnote{Nigerian Communications Act, 2003, s.1.} Consequently, the Act does provide for matters concerning cybercrime. For instance, the Act makes it an obligation on the part of telecommunication providers to ensure that their network or facilities are not used to perpetrate crime. Section 146(1) of the Act states:

\begin{itemize}
  \item Preventing the use of facilities to commit cybercrimes.
  \item Complying with all other legal requirements.
\end{itemize}
A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content application service that he provides from being used in, or in relation to, the commission of any offence under any law in operation in Nigeria.78

The prevention of “the commission of any offence under any law in operation in Nigeria” also includes the cybercrime offences provided under the Cybercrimes (Prohibition, Prevention Etc) Act 2015 which has been in operation since 15 May 2015. Moreover, it is the obligation of telecommunications service providers to give assistance to the Nigerian Communications Commission (NCC) or any other authority on reasonable grounds for the purpose of preventing the commission or attempted commission of an offence under any written law in operation in Nigeria or otherwise in enforcing the laws of Nigeria, including the protection of the public revenue and preservation of national security.79 Criminal liability accrues to a telecommunications provider where there is lack of fulfillment of the aforementioned obligations but where any such act or omission is done in good faith in the performance of the aforesaid obligations, liability in any criminal proceedings for any damage shall not lie.80

In addition, the Act authorizes the NCC to determine whether or not telecommunications service providers shall implement the capability to allow authorized interception of communications pursuant to specified technical requirements for such authorized interception capability.81 Upon the occurrence of any public emergency or in the interest of public safety, the NCC may give an order mandating that any communication or class of communications to or from any Service provider, person or the general public, relating to any specified subject shall not be communicated or shall be intercepted or detained; or that any such communication or its records shall be disclosed to an authorized officer.82 In consultation with the authorities specified by NCC, NCC may direct telecommunications service providers to develop, a disaster plan for the survivability and recovery of any services or network facilities in case of a disaster, crisis or civil emergency.83

2.7 Evidence Act 2011.
Predominantly, at play in Cybercrime cases coming before courts, are electronic and computer generated documents of various kinds. It is a generic description for certain classes of evidence processed, stored or derived from computers or computer based devices or electronic communication systems. A major characteristic of this class of documents is that unless printed, they are paperless and though contained in tangible objects are visible but intangible. These include; e-mails, telephone records, text messages, digital cameras, mobile phones, letters or other

78 Ibid., s.146(1). Emphasis is mine.
79 Ibid., s.146(2).
80 Ibid., s.146(3).
81 Ibid. s.147.
82 Ibid., s.148(1)(c).
83 Ibid., s.149.
documents processed in a computer or electronic device or stored in a computer based storage device etc.  

The issue of admissibility of evidence is crucial to cybercrime prosecution as it has the capacity to determine the outcome of a case one way or the other. How particular legal personnel’s and courts treats such evidence is of utmost significance. A case may be won or lost on the strength of a particular piece of evidence that has been admitted or rejected, as the case may be. The Evidence Act 2011 allows the admissibility of electronic evidence elicited for the prosecution of cyber criminals in Nigerian courts. Specifically, section 84 of the Evidence Act 2011 is a plus to effective cybercrime prosecution in Nigeria because of its recognition of the admissibility of the aforementioned electronic or computer generated evidence in trials and the enlargement of the definition of documents to include computer generated ones by the Nigerian Evidence Act 2011.

However, the admissibility of the aforementioned electronic or computer generated evidence in cybercrime trials is subject to the fulfillment of certain conditions. Section 84 of the Act states that provided it can be established that the document sought to be tendered was produced by the computer from information supplied to it during a period over which the computer was used regularly and functioning properly to store and process information for the purpose for which that document was produced at that particular time, any statement contained in such document shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, in any proceedings.

2.8 National Information Technology Development Agency (NITDA) Act 2007

The prevalence of criminality through the medium of Information and Communication Technology was regarded as science fiction in Nigeria a few years ago, but today, the Nigerian polity is grappling with the realities of the menace of cyber criminality in the 21st Century. There is the attendant growth of electronic communication which is by far the most reliable form of communication in the area of business and social interaction probably because it is permanent, nearly indestructible and the ease of transfer. Resort have been made to E-mail, Blackberry Messenger, Yahoo Messenger and even text messages in negotiations, settlement discussions, confidential communications, transaction closings and the completion of contracts for goods and services. Obviously, I cannot rule out the

85 Ibid.
86 Ibid; Evidnece Act 2011, s.s 84 & 258. S.258 provides “A document includes- (a) books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter; (b) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it, and (c) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; (d) any device by means of which information is recorded, stored or retrievable including computer output.”
87 Ibid.; See generally, Nigerian Evidence Act, 2011, s.84(1) (2)&(4); see also 90(1)(a) & (d).
contribution of these fascinating technologies in our lives, both personally and professionally.\textsuperscript{88} Criminals in Nigeria are using these high end technologies to commit cybercrimes which ordinarily are beyond reach and understanding of a layman. These crimes involve the use of information technology infrastructure, including illegal access, illegal interception, data interferences, system interferences, forgery (ID theft) and electronic fraud etc.\textsuperscript{89}

Nevertheless, a body known as the National Information Technology Development Agency was established by the National Information Technology Development Agency (NITDA) Act 2007\textsuperscript{90} to plan, develop and promote the use of Information technology in Nigeria. The NITDA Act amongst others empowers the Agency to Create a frame work for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria; Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information; Develop guidelines for the networking of public and private sector establishment; Render advisory services in all information technology matters to the public and private sectors; Determine critical areas in Information Technology requiring research intervention and Development in those areas; Advice the Government on ways of promoting the development of information technology in Nigeria including introducing appropriate information technology legislation, to enhance national security and vibrancy of the industry; and accelerate internet and intranet penetration in Nigeria and promote sound internet.\textsuperscript{91}

If the mandate given to NITDA is efficiently and effectively carried out, cybercriminals in Nigeria will not have a field day in engaging in cybercrime offences through Information and Communication Technology.

2.9 Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime within ECOWAS

Nigeria is a member state of the ECOWAS. ECOWAS recognizing the fact that the use of information and communication technologies and the internet has generated an upsurge of reprehensible acts; that such criminality require the identification of a legal regime and a suitable punishment because of the level of damage they generate; and the need to adopt a framework for criminal liability for the purpose of fighting cybercrime effectively, at her sixty-sixth ordinary session of the council of ministers issued a directive on fighting cybercrime within ECOWAS and urged member states to adopt necessary legislative, regulatory and administrative measures to comply.\textsuperscript{92}

\textsuperscript{88} F.E. Eboibi, (n.83)
\textsuperscript{89} Ibid.
\textsuperscript{90} National Information Technology Development Agency Act 2007, Explanatory Memorandum.
\textsuperscript{91} Ibid., s.6.
\textsuperscript{92} ECOWAS sixty-sixth ordinary session of the council of ministers Directive C/DIR. 1/08/11 on fighting cybercrime within ECOWAS; preambles 10-13; art. 35
The ECOWAS directive is made up of Chapters I to VII and Articles 1 to 35. Chapter 1 encompasses general provisions, which include article 1 – definitions; article 2 – objective of the Directive geared towards adapting a substantive criminal law and the criminal procedure of ECOWAS Member States to address the menace of cybercrime.\footnote{Ibid., art. 2.} Article 3 contains the scope of the Directive, basically applicable to all cyber-related offence within the ECOWAS sub-region.\footnote{Ibid., art.3} Chapter II and III provides for offences: fraudulent access to computer systems;\footnote{Ibid., art.4} fraudulently remaining in a computer system;\footnote{Ibid., art.5} interfering with the operation of a computer system;\footnote{Ibid., art.6} fraudulent input of data in a computer system;\footnote{Ibid., art.7} fraudulent interception of computer data;\footnote{Ibid., art.8} fraudulent modification of computer data;\footnote{Ibid., art.9} computer data forgery;\footnote{Ibid., art.10} obtaining benefit from computer related fraud;\footnote{Ibid., art.11} fraudulent manipulation of personal data;\footnote{Ibid., art.12} use of forged data;\footnote{Ibid., art.13} obtaining equipment to commit an offence;\footnote{Ibid., art.14} participation in an association or agreement to commit computer offence;\footnote{Ibid., art.15} production of child pornography or pornographic representation;\footnote{Ibid., art.16} import or export of child pornography or pornographic representation;\footnote{Ibid., art.17} possession of child pornography or pornographic representation;\footnote{Ibid., art.18} facilitation of access of minors to pornography, documents, sound or pornographic representation;\footnote{Ibid., art.19} possession of racist or xenophobic written documents or pictures through a computer system;\footnote{Ibid., art.20} threat through a computer system;\footnote{Ibid., art.21} abuse through a computer system;\footnote{Ibid., art.22} denying or justifying acts or crimes against humanity by means of a computer system;\footnote{Ibid., art.23} aggravating circumstances of common law offences;\footnote{Ibid., art.24} violations of computer data, software and programme;\footnote{Ibid., art.25}
offence committed through electronic means of communication.\textsuperscript{117} Chapter IV contains sanctions or penalties for breaching the aforementioned offences under the Directive, specifically, articles 28 and 29.\textsuperscript{118} Chapter V encompasses rules of procedure. These include search or access to a computer;\textsuperscript{119} expedited preservation of data;\textsuperscript{120} method of proof;\textsuperscript{121} and judicial cooperation.\textsuperscript{122} Chapter VII is the final provisions, which contains publication\textsuperscript{123} and implementation.\textsuperscript{124}

2.10. **African Union Convention on Cybersecurity and Personal Data Protection**
Nigeria is also a member state of the African Union (AU). The AU on 27 June 2014, at her 23\textsuperscript{rd} session of the summit of the AU in Malabo, Equatorial Guinea adopted the AU Convention on Cybersecurity and Personal Data Protection, wherein member states were urged to adopt legal measures to curb cybercrime.\textsuperscript{125} However, the AU Convention is yet to enter into force because the requisite 15 countries ratification clause has not been achieved till date.\textsuperscript{126}

3. **Conclusion**
This paper has highlighted the positive impact the development of computers; information communication infrastructure and the internet have brought to Nigerians and the Nigerian polity, both from the professional and personal perspectives. There is no gainsaying that despite the acclaimed positives, some persons with criminal intent have also capitalized on these developments to perpetrate cybercrime against cybercitizens. The proliferation of cyber criminality in Nigeria raised a debate in the literature, questioning the availability or otherwise of applicable laws to investigate and prosecute perpetrators of cybercrime. Although, prior to the enactment of the Nigerian Cybercrimes (Prohibition, Prevention, etc) Act 2015 there was no comprehensive cybercrime law put in place to investigate and prosecute cybercrime perpetrators. However, with the commencement of the Act on 15 May 2015, Nigeria has now joined nations with comprehensive law to investigate and prosecute cybercriminals. Apart from examining the Nigerian Cybercrimes Act as an applicable law, this paper has also looked at other derivable sources of law within the reach of stakeholders; law enforcement agents; prosecutors; counsel to eradicate cybercrime in Nigeria. This paper has consequently filled the gap in the literature by examining the aforementioned legislations and case laws, thereby putting to rest the debate whether or not there exists applicable laws to investigate and prosecute perpetrators of cybercrime in Nigeria.

\textsuperscript{117} Ibid., art.26
\textsuperscript{118} Ibid., art.28 & 29
\textsuperscript{119} Ibid., art.30
\textsuperscript{120} Ibid., art.31
\textsuperscript{121} Ibid., art.32
\textsuperscript{122} Ibid., art.33
\textsuperscript{123} Ibid., art.34
\textsuperscript{124} Ibid., art.35.
\textsuperscript{125} AU Convention on Cybersecurity and Personal Data Protection, art. 25
\textsuperscript{126} Ibid, art. 36.