ELECTRONIC COMMUNICATION INFRASTRUCTURE INNOVATION: IS NIGERIA THE HUB OF CYBERCRIME AND CYBERCRIME PERPETRATORS?

Felix E. Eboibi*

Abstract

Prior to the signing of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 by former President, Dr Goodluck Ebele Jonathan on 15 May 2015, which is currently the legal framework for cybercrime enforcement in Nigeria, commentators, in domestic and international reports labeled Nigeria as the hub of cybercrime and cybercrime perpetrators. This paper questions the rationale and the veracity or otherwise of the assertion "Nigeria is the hub of cybercrime and cybercrime perpetrators" and in response, posits two models i.e the Myopic or Constitutional Law Model and the Comprehensive Law Model. The Myopic or Constitutional Law Model basically examines the lack of prior cyber law and poor global rating of Nigeria in cybercrime perpetration as the basis for the conclusion reached by the literature that Nigeria is the hub of cybercrime and cybercrime perpetrators and against the backdrop justify that the basis is one-sided and have been whittled down

* Ph.D, LL.M(Nig.), LL.B(Cal.), B.L(Nigerian Law School, Abuja), Lecturer, Faculty of Law, Niger Delta University, Wilberforce Island, Nigeria. E-mail: lixboibi@yahoo.com or felixeboibi@mail.ndu.edu.ng. I wish to acknowledge and appreciate Mr Prince Madojemu for his enormous assistance towards the collection of the data used for this research work from EFCC. See generally, F.E Eboibi, Enforcement of Cybercrime in Nigeria: Are We Still Having Teething Problems? Being a paper presented in a Certificate Training Course/Conference; *Cybersecurity, Sovereignty, and Democratic Governance in Africa* organized by the Council for the Development of Social Science in Africa, Democratic Governance Institute, Dakar, Senegal, 27 July 2015 – 7 August 2015.

by the Comprehensive Law Model. While the Comprehensive Law Model on the other hand, portends to show that in the absence of a prior cyber law, Nigeria through the Economic and Financial Crimes Commission (EFCC) recorded positive achievements in cybercrime enforcement and that the basis for the conclusion is misconceived on the premise that there is lack of available literature on the prosecutorial efforts and numerous convictions recorded against cybercrime perpetrators in Nigeria. In the final analysis, this paper argues that Nigeria is not the hub of cybercrime and cybercrime perpetrators.

Introduction

According to recent reports, Nigeria has an estimated population of 177,155,754 million people[1] and the largest population of telecommunication subscribers in Africa with more than 140 Million subscribers.[2] Nigeria also has the largest Internet user population in Africa.[3] The corollary is that there is the attendant growth of electronic communication which appears to be a reliable form of communication in the area of business and social interaction probably because it is a permanent, nearly indestructible and comes with the ease of transfer. Nigerians use e-mail, blackberry messenger, yahoo messenger and even text messages in negotiations, settlement discussions, confidential communications,

---

[1] See Wikipedia, 'List of Countries by number of Mobile Phone users', <http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use> Last accessed 23 April 2015.

[2] Budde Comm, Nigeria – 'Mobile Market - Insights and Statistics,' available at <**http://www.budde.com.au/Research/Nigeria-Mobile-Market-Insights-and-Statistics.html>** Last accessed 23 April 2015.

[3] Internet World Stats, Usage and Population Statistics, available at <http://www.internetworldstats.com/africa.htm> Last accessed 23 April 2015.

transaction closings and the completion of contracts for goods and services, researches have now been made easier and faster.[4]

However, the deregulation of the Telecom Sector and introduction of the National Policy on Information Technology (NPFIT) policy was quickly followed by criminals utilizing the internet to perpetrate all manner of fraud. There are different categories of fraud that became commonly perpetrated on-line viz; electronic auction or retail-based fraud schemes, stock scams, work at home scams and on-line (e-mail) advance fee fraud scams. The advance fee e-mail scheme is the most costly form of internet fraud from the Nigerian perspective. The messages are often referred to as "Nigerian" or "419" cyber scams because the emails often come from individuals who purport to reside in a foreign country - Nigeria. The messages are presented as emanating from individuals who claim to need assistance moving a large sum of money out of Nigeria or any other country. If the response is positive, the sender would then begin a systematic extraction of money from the victim to be transferred to a designated bank account usually through Western Union. Most times, such monies are meant to cover "official fees" or "attorney fees". If the victim is naïve, the perpetrator will end up sweeping his bank account clean before realizing that he/she has been duped.[5]

Anyone unskilled in this art cannot fancy tracing the root of the crime. It has culminated into a new term called "cybercrime." It is a crime in which the computer is either used as a tool or target or

---

[4] F.E. Eboibi, 'Cybercrime Prosecution and the Nigerian Evidence Act, 2011: Challenges of Electronic Evidence' (2011) 10 *Nigerian Law and Practice Journal*, 139 at 140.

[5] Thomas J. Holt & Danielle C. Graves, 'A Qualitative Analysis of Advance Fee Fraud E-mail Schemes' (2007) 1(1) *International Journal of Cyber Criminology,* available at <http://www.cybercrimejournal.com/thomas&danielleijcc.htm> Last accessed 20 April 2015 & Taiwo A. Oriola, 'Advance Fee Fraud on the Internet: Nigeria's Regulatory Response' (2005) 21 *Computer Law & Security Report,*, 237 at 239-240.

involving information technology infrastructure, including illegal access, illegal interception, data interference, forgery (ID theft and electronic fraud etc). Prior to 2001, the term cybercrime was not one that could have been used in the same sentence with Nigeria because Nigeria as a country was just a crawling toddler at that time with respect to computers and internet. However, that toddler learnt to walk, jump, run and even fly, because cybercriminals have increased, coming up with ingenious new ways to trick people out of the money in their pockets. These criminal activities have created illegitimate wealth for some Nigerians while it adversely affects the Nigerian economy and external image.[6]

Consequently, commentators, in domestic and international reports have referred to Nigeria as the hub of cybercrime and cybercrime perpetrators. This accusation has galvanized Nigeria into reacting against such an embarrassing international reputation.[7] This work

---

[6] Nuhu Ribadu, 'Cybercrime and Commercial Fraud: A Nigerian Perspective', (Modern Law for Global Commerce Congress to celebrate the fortieth annual session of UNCITRAL, Vienna, 9 – 12 July 2007) available at <http://www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf> Last accessed 10 April 2015 & Roseline Obada Moses-Oke, 'Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT),' (May 30 2012) vol. 12 *Journal of Philosophy, Science & Law*, available at <www.miami.edu/ethics/jpsl> Last accessed 20 April 2015.

[7] Wolf Pack & Digital Jewels, 2014: 'The Nigerian Cyber Threat Barometer Report',4,6, available at <https://www.digitaljewels.net/index.php/resource-center/djlnews/129-the-2014-nigerian-cyber-threat-barometer> Last accessed 4 April 2015; ALoucif Kharouni, 'Africa: A New Safe Harbor for Cybercriminals?' Trend Micro Incorporated Research Paper, 2013, 1, available at <http://www.trendmicro.nl/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf> Last accessed 10 April 2015; E.E Adomi & S.E. Adomi, 'Combating Cybercrime in Nigeria' (2008) vol.26(5) *The Electronic Library,* 718; Internet Crime Complaint Center, 2010 *Internet Crime Report* (National White Collar Crime Complaint Center: United States, 2011), 11, available at <http://www.nw3c.org or www.ic3.gov> Last accessed 9 April 2015; Seun Ayantokun, 'Nigeria needs Anti-Cybercrime Law now – Minister' (Tuesday 15 November 2011), available at

questions the rationale and the veracity or otherwise of the assertion "Nigeria is the hub of cybercrime and cybercrime perpetrators." Is it absolutely correct to assert that Nigeria is the hub of cybercrime and cybercrime perpetrators? In response, this work posits two models i.e the Myopic or Constitutional Law Model and the Comprehensive Law Model.

The grouse of the Myopic or Constitutional Law Model is hinged on; (1) Lack of prior Cyber Law in Nigeria and (2) The poor global rating of Nigeria in terms of cybercrime perpetration. From this perspective, a crime is not a crime unless it is codified. Hence, for perpetrators of cybercrime to be prosecuted, such criminal acts complained of must have been defined as criminal and punishable by a written law in Nigeria. The contrary amounts to a flagrant abuse of the fundamental rights to fair hearing of the perpetrator sought to be tried.[8] Proponents have also furthered their arguments as a result of the inability of Nigeria through her National Assembly to enact several Bills presented before the House prior to 2015.[9] Moreover, based on the global rating, Nigeria has always been in number one position in Africa and either number two or

---

<http://www.tribune.com.ng/index.php/tele-info/31205-nigeria-needs.anti-cyber-crime-law-now-minister> Last accessed 3 April 2015; L. Agih & B. Mibzar, 'Nigeria: Cybercrimes-Nation Ranks Third in the World' (3 February 2010), available at <http://www.alafrica.com/nigeria> Last accessed 2 April 2015; Eric Agwe-Mbarika Akuta, *et.al*, 'Combating Cyber Crime in Sub-Saharan Africa: A Discourse on Law, Policy & Practice' (May 2011) vol.1(4) *Journal of Research in Peace, Gender and Development,* 129,132; Okonigene Robert Ehimen & Adekanle Bola, 'Cybercrime in Nigeria' (2009) vol.3(1)*Business Intelligence Journal,* 95,97; Roseline Obada Moses-Oke, (n.6) 11.

[8] Constitution of the Federal Republic of Nigeria, 1999 (As Amended), s. 36(8) &(12)

[9] Computer Security and Critical Information Infrastructure Bill 2005; Cyber Security and Data Protection Agency Bill 2008; Electronic Fraud Protection Bill 2008; Nigeria Computer Security and Protection Agency Bill 2009; Computer Misuse Bill 2009; Economic and Financial Crimes Commission Act(Amendment) Bill 2010; Cyber Security Bill 2011 & Cybercrime Bill 2013.

three between 2002 and 2013 globally.[10] In whole, perpetrators of cybercrime in Nigeria had a field day since they were not being prosecuted as a result of the absence of a prior Cyber Law. For instance, Taiwo A. Oriola stated that 'there has not been a single reported conviction of any of the alleged perpetrators of advance fee fraud schemes in cyberspace from Nigeria'.[11] This work advocates that the inference drawn from the Myopic or Constitutional Law Model is misplaced. The nicknaming of Nigeria as a hub of cybercrime and cybercrime perpetrators is more or less accentuated by a general lacuna or absence in the literature about the numerous convictions recorded by the Nigerian Government against cybercrime perpetrators.

The Comprehensive Law Model argues that in the absence of a prior Nigerian Cyber Law, Law enforcement agents found solace in the Economic and Financial Crimes Commission (EFCC) Act, 2004 and the Nigerian Advance Fee Fraud and Other Fraud Related Offences Act, 2006 to investigate and prosecute perpetrators of On-line Advance Fee Fraud and other fraud related crimes. The EFCC at the helm of affairs devised quite a number of measures which yielded positive results towards enforcing cybercrime in Nigeria. Considering, the absence in the literature of the nature and/or number of convictions with instances that have been recorded by EFCC, this work further examines these as it relates to the superior courts of record (i.e High Courts, Federal High Courts, Court of Appeal and Supreme Court).

This work further answers the question; what measures were undertaken by EFCC to eradicate cybercrime in Nigeria which contributed to the recording of numerous convictions in the superior courts of record (i.e High Courts, Federal High Courts, Court of Appeal and Supreme Court) prior to the enactment of the

---

[10] Internet Crime Complaint Center, 2010 – 2013 *Internet Crime Report* (National White Collar Crime Complaint Center: United States, 2002 - 2013), available at <http://www.nw3c.org or www.ic3.gov> 9 April 2015.

[11] Taiwo A. Oriola, (n.5) at 247.

Nigerian Cybercrimes Act 2015? In this regard, numerous convictions were recorded in the superior courts of record (i.e High Courts, Federal High Courts, Court of Appeal and Supreme Court). Based on the foregoing, this work summarily concludes by articulating the true position of Nigeria in terms of the enforcement of cybercrime through the EFCC as opposed to Nigeria being a hub of cybercrime and cybercrime perpetrators.

Myopic or Constitutional Law Model

This section basically examines the basis of the conclusion reached by the literature that Nigeria is the hub of cybercrime and cybercrime perpetrators and against the backdrop justify that the basis is one-sided and have been whittled down by the Comprehensive Law Model.

This model is borne out of the rule of law, which simply means that law rules or reigns. It is a situation where things are done in accordance with law thereby excluding any form of arbitrariness. Thus in *Re Mohammed Olayori and Others,*[12] the learned High Court Judge said: 'If we are to have our actions guided and restrained in certain ways for the benefit of society… then whatever status, whether post we hold, we must succumb to the rule of law. The alternative is anarchy and chaos.' The corollary is that a man can only be punished for contravening the law and not for anything else.

In consonance with the rule of law, the Constitution of the Federal Republic of Nigeria, 1999(as amended) provides for the preservation of rights and fair hearing is guaranteed in all trials in respect to persons. Specifically, provisions regarding the treatment of criminal suspects upon arrests for the commission of offences i.e rights to hearing and fair trials have been incorporated in section 36 of the 1999 Nigerian Constitution. In recognition of these, cybercrime legislation ought to have been put in place prior to the

[12] (1969)1 NMLR 236.

enactment of the Cybercrimes Act 2015 to prevent perpetrators and to ensure that these crimes are not tolerated and when they occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter them and others from cybercrime. These presuppose the prior enactment of well defined cybercrime offences for use in prosecuting cyber criminals in Nigeria.[13]

This is germane because in an attempt to prosecute perpetrators of cybercrime, such criminal acts complained of must have been defined as criminal and punishable by a written law in Nigeria. Any deviation amounts to a flagrant abuse of the fundamental right to fair hearing of the person so tried. Practices of these are not permitted in a Nigerian democratic society that is subject to rule of law and due process.[14] Section 36(8) & (12) of the Constitution of the Federal Republic of Nigeria 1999 (as amended) stipulates thus:

> (8) No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place constitute such an offence…(12) Subject as otherwise provided by this Constitution, a person shall not be convicted of a criminal offence unless the offence is defined and the penalty therefore is prescribed in a written law; and in this subsection a written law refers to an Act of National Assembly or a law of a State, any subsidiary legislation or instrument under the provision of a law.[15]

---

13 F. E Eboibi, 'Cybercrime Prosecution and the Nigerian Evidence Act, 2011: Challenges of Electronic Evidence', Being a paper presented at the 2013 International Digital & Mobile Forensics Conference at Public Service Institute of Nigeria, Abuja, Nigeria 12-14 Nov. 2013, 4; Laura Ani, 'Cyber Crime and National Security: The Role of the Penal and Procedural Law', (nails-nigeria.org/pub/lauraani.pdf) 10 July 2013.

14 Ibid.

15 Constitution of the Federal Republic of Nigeria, 1999 (As Amended), s. 36(8) &(12); See also the Nigerian Criminal Procedure Act, Cap. C41 Laws

In *Chief Olabode George vs Federal Republic of Nigeria*,[16] the appellant was, at all material times, the Chairman of the Board of Directors of Nigeria Ports Authority. He was charged before the trial court along with others to have exceeded the limit set to their authority to award contracts and contrived to bring the contracts within their limits by splitting them while also inflating their prices. The trial court found him guilty and was convicted for abuse of office by splitting contracts, conspiracy and disobedience of lawful orders by splitting contracts. Dissatisfied with the High Court judgment, the appellant appealed to the Court of Appeal where the trial judgment was affirmed. On further appeal to the Supreme Court, the court while discharging and acquitting the accused held thus:

> It is clear from the reproduced portion of Exhibit P3, as above, that it contains guideline which forbids splitting of contracts by any officer. It stipulates that breach of same shall be met with disciplinary action. This may be in form of administrative action against an officer who breaches the rules. Disobeying Exhibit P3 is not made an offence by any Act of the National Assembly or law of a State House of Assembly or even the contents of Exhibit P3 itself. Even then, disobedience of Exhibit P3 is nowhere penalized in a written law. **Any conduct that must be sanctioned must be expressly stated in a**

---

of the Federation of Nigeria 2004, s. 151(3) – it states that a charge against a suspect must contain the "written law" prohibiting the act and the section, otherwise, the charge is void. See also *Omoju vs. Federal Republic of Nigeria* (2008) 7 NWLR pt. 1085, 38; *George vs Federal Republic of Nigeria* (2011) All FWLR pt. 587, 664; *Amadi vs. Federal Republic of Nigeria* (2011) All FWLR pt. 561, 1588; In *Aoko v. Fagbemi* the court *held; inter-alia* that nobody could be punished for an offence that was not part of our written laws at the time it was committed.

16 (2013) LPELR-21895(SC). Suit No. SC. 180/2012, Supreme Court Judgment delivered on 13 December 2013 available at <lawpavilionpersonal.com/ipad/books/21895.pdf> Last accessed 11 July 2015.

> **written law to wit: an Act by the National Assembly. That is what section 36 (12) of the 1999 Constitution provides**. Such conduct should not be left to conjecture. As well, it cannot be inferred by the court. It occurs to me that section 203 of the Criminal Code is not in tune with the dictate of section 36 (12) of the 1999 Constitution. That being the position, the charges filed under section 203 of the said Code ostensibly for splitting contract in disobedience of lawful order by constituted authority cannot stand.[17]

The Supreme Court stated further:

> It occurs to me that the entire proceedings ran foul of the provisions of section 36 (8) of the 1999 Constitution which provides that;- "No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence, and no penalty shall be imposed for any criminal offence heavier than the penalty in force at the time the offence was committed." The respondent, in a way, appreciates the above salient points by its own action in putting in place the Public Procurement Act, 2007 on the 1st June, 2007 which contains in it's section 58 penal sanctions for splitting of tenders. The law was not made with retrospective effect. It could not have been so in the face of the clear provision of section 36 (8) of the 1999 Constitution. This court, as the guardian of the Constitution, will not allow such to happen.[18]

[17] Ibid, emphasis mine.
[18] Ibid

The foregoing, implies that a crime is not a crime unless it is codified otherwise it is more or less condemned moral wrongs and sociologically perceived as social vices. In recognition of this, the Nigerian National Assembly prior to the enactment of the Cybercrimes (Prohibition, Prevention Etc) Act, 2015 made several attempts to enact a Cyber Law to eradicate cybercrime in Nigeria through the consideration of bills[19] brought before them.

However, the *lacuna* provided by the absence of a prior cyber law in Nigeria made commentators, local and international to assert that Nigeria is the hub of cybercrime and cybercrime perpetrators. They reasoned that perpetrators of cybercrime in Nigeria were not being prosecuted thereby resulting to the proliferation of cybercrime. For instance, Okonigene Robert Ehimen & Adekunle Bola,[20] argued about the damaging nature of cybercrime in Nigeria and questions the effort of the EFCC in respect to the prosecution of cybercrime perpetrators. They stated that no serious impact has been made by EFCC towards the arrest and prosecution of cybercrime perpetrators and concluded 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; Dr. Dejo Olowu,[21] recognized the growth of cybercrime perpetuation in Nigeria and attributed same to the lack of internet specific laws and decried the efforts of law enforcement agencies towards eradicating cybercrime as neither effective nor sustainable; Roseline Obada Moses-Oke, blamed the current state of cyber criminality on the inability of NPFIT to put in

---

19 Computer Security and Critical Information Infrastructure Bill 2005; Cyber Security and Data Protection Agency Bill 2008; Electronic Fraud Protection Bill 2008; Nigeria Computer Security and Protection Agency Bill 2009; Computer Misuse Bill 2009; Economic and Financial Crimes Commission Act(Amendment) Bill 2010; Cyber Security Bill 2011 & Cybercrime Bill 2013.

20 Robert Ehimen & Adekanle Bola, (n.6).

21 Dr. Dejo Olowu, 'Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa'(2009) 1 *Journal of Information, Law & Technology*, pp.6,8.

place a Cyber law before the commencement or during the implementation of ICT policy in Nigeria.[22]

Moreover, commentators also hinged their arguments on the poor global rating of Nigeria in cybercrimes perpetration. In 2002 the Internet Fraud Complaint Centre published a report which established that Nigeria was ranked second (2nd) in the world among top ten countries and first (1st) in Africa in cybercrime perpetration with a rating of 5.1 percent; United States of America(USA) is first (1st) with 76.7 percent rating, followed by Canada second(2nd) with 3.5 percent rating.[23] In 2003 the Internet Crime Complaint Centre(IC3) ranked Nigeria third (3rd) in the world among top ten countries and first(1st) in Africa in cybercrime perpetration with a rating 2.9 percent, USA is first(1st) with 76.4 percent rating, followed by Canada second(2nd) – 3.3 percent;[24] the 2004 report ranked Nigeria third(3rd) in the world among top ten countries and first (1st) in Africa in cybercrime perpetration with 2.87 percent, USA is first (1st) with 78.75 percent, followed by Canada second(2nd) with 3.03 percent;[25] the 2005 report ranked Nigeria second(2nd) in world among top ten countries and first(1st)

---

22 Roseline Obada Moses-Oke, (n.6).

23 National White Collar Crime Center and the Federal Bureau of Investigation, IFCC 2002 Internet Fraud Report January 1, 2002—December 31, 2002, (The National White Collar Crime Center, 2003), p.8, available at <http://www.ic3.gov/media/annualreport/2002_IC3Report.pdf> Last accessed 10 July 2015.

24 National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2003 Internet Fraud Report January 1, 2003-December 31, 2003,p.9, available at <http://www.ic3.gov/media/annualreport/2003_IC3Report.pdf> Last accessed 10 July 2015.

25 National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2004 Internet Fraud - Crime Report, 1 January2004 - 31 December 2004, (The National White Collar Crime Center, 2005), p.10, available at <http://www.ic3.gov/media/annualreport/2004_ic3report.pdf> Last accessed 10 July 2015.

in Africa with 7.9 percent in cybercrime perpetration, USA is first (1st) with 71.2 percent, United Kingdom is third(3rd) with 4.2 percent;[26] the 2006 report ranked Nigeria third(3rd) in world among top ten countries and first(1st) in Africa with 5.9 percent in cybercrime perpetration, USA is first (1st) with 60.9 percent, followed by United Kingdom second(2nd) with 15.9 percent;[27] the 2007 report ranked Nigeria third(3rd) in world among top ten countries and first(1st) in Africa with 5.7 percent in cybercrime perpetration, USA is first (1st) with 63.2 percent, followed by United Kingdom second(2nd) with 15.3 percent;[28] the 2008 report ranked Nigeria third(3rd) in world among top ten countries and first(1st) in Africa with 7.5 percent in cybercrime perpetration, USA is first (1st) with 66.1 percent, followed by United Kingdom second(2nd) with 10.5 percent;[29] the 2009 report ranked Nigeria third(3rd) in world among top ten countries and first(1st) in Africa with 8.0 percent in cybercrime perpetration, USA is first (1st) with 65.4 percent, followed by United Kingdom second(2nd) with 9.9 percent;[30] the 2010 report ranked Nigeria third(3rd) in world among top ten countries and first(1st) in Africa with 5.8 percent in

---

[26] National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2005 Internet Fraud - Crime Report, 1 January 2005 - 31December 2005, p.11, available at <http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf> Last accessed 10 July 2015.

[27] National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2006 Internet Fraud - Crime Report, 1 January 2006 – 31 December 2006, p.11, available at <http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf> Last accessed 10 July 2015.

[28] National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2007 Internet Fraud - Crime Report, 1 January 2007 - 31 December 2007,p.10, available at <http://www.ic3.gov/media/annualreport/2007_ic3report.pdf> Last accessed 10 July 2015.

[29] National White Collar Crime Center, 2008 Internet Crime Report, p.8, available at <http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf> Last accessed 10 July 2015.

cybercrime perpetration, USA is first (1st) with 65.9 percent, followed by United Kingdom second(2nd) with 10.4 percent;[31] the 2011 report did not rank countries per perpetration rather by individual complaints received, among top ten countries ranked, Nigeria was nowhere to be found, USA first(1st) with 90.99 percent, followed by Canada second(2nd) with 1.44 percent, South Africa seventh(7th) with) 0.22 percent;[32] the 2012 report was also based on complaints received, among 50 countries, Nigeria was ranked twenty fifth (25th) globally and first in Africa with 0.08 percent, USA is first(1st) with 91.19 percent, followed by Canada second(2nd) with 1.43 percent;[33] the 2013 report was based on complaints received, among 50 countries, Nigeria was ranked third (3rd) globally and first in Africa with 1.37 percent, USA is first(1st) with 31.89 percent, followed by United Kingdom second(2nd) with 1.72 percent;[34] the 2014 report was based on complaints received, among 50 countries, Nigeria was ranked twenty fourth (24th) globally and second in Africa with 0.08 percent (South Africa is

---

30 National White Collar Crime Center, 2009 Internet Crime Report, p.9, available at <http://www.ic3.gov/media/annualreport/2009_ic3report.pdf> Last accessed 10 July 2015.

31 National White Collar Crime Center, 2010 Internet Crime Report, p.12, available at <http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf> Last accessed 10 July 2015.

32 National White Collar Crime Center, 2011 Internet Crime Report, p.10, available at <http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf> Last accessed 10 July 2015.

33 National White Collar Crime Center, 2012 Internet Crime Report, p.25, available at <http://www.ic3.gov/media/annualreport/2012_ic3report.pdf> Last accessed 10 July 2015.

34 National White Collar Crime Center, 2013 Internet Crime Report, p.21, available at <http://www.ic3.gov/media/annualreport/2013_ic3report.pdf> Last accessed 10 July 2015.

first in Africa with 0.16 percent), USA is first(1st) with 91.54 percent, followed by Canada second(2nd) with 1.51 percent.[35]

Table 1: Representation of Nigeria's Ranking in Cybercrime Source: Internet Cybercrime Report from 2002 - 2014

YEAR	GLOBAL RANKING	AFRICA RANKING
2002	Second(2nd)	First (1st)
2003	Third (3rd)	First (1st)
2004	Third (3rd)	First (1st)
2005	Second(2nd)	First (1st)
2006	Third (3rd)	First (1st)
2007	Third (3rd)	First (1st)
2008	Third (3rd)	First (1st)
2009	Third (3rd)	First (1st)
2010	Third (3rd)	First (1st)
2011	Not ranked among top ten	-
2012	Twenty fifth(25th)	First (1st)
2013	Third (3rd)	First (1st)
2014	Twenty fourth	Second(2nd)

Again, Eric Agwe-Mbarika, *et.al,*[36] Loucif Kharouni,[37] demonstrated that Sub-Sahara Africa, particularly Nigeria is a safe haven for cyber criminality. They drew conclusion from Nigeria's rating as 3rd globally and 1st in Africa and the absence of a prior Cyber law.

---

[35] National White Collar Crime Center, 2014 Internet Crime Report, p.22, available at <http://www.ic3.gov/media/annualreport/2014_ic3report.pdf> Last accessed 10 July 2015.

[36] Eric Agwe-Mbarika Akuta, *et.al*, (n.7).

[37] Africa: A New Safe Harbor for Cybercriminals? Trend Micro Incorporated Research Paper, 2013,p.1, available at <http://www.trendmicro.nl/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf> Last accessed 10 April 2015.

It is submitted that the basis for the conclusion that Nigeria is the hub of cybercrime and cyber criminality on ground of lack of prior cyber law and the poor global rating of Nigeria in cybercrime perpetration by the aforementioned domestic and international literature is seriously flawed. No doubt, Nigeria had no cyber law before now and was rated poorly globally in terms of cybercrime perpetration but that is not enough to tag Nigeria as the hub of cybercrime or safe haven for cyber criminality.

It must be noted that the 2002 – 2014 Internet Crime Reports rating or ranking of cybercrime perpetration were mostly based on fraud related acts; Nigerian Letter Fraud, 419 fraud, 419 scams, online/419 advance fee fraud, romance scams, debit and credit fraud.[38] These incidents formed part of the basis of Nigeria's poor ranking. The literature is bereft of the fact that despite the absence

[38] National White Collar Crime Center and the Federal Bureau of Investigation, IFCC 2002 Internet Fraud Report, 1 January 2002 – 31 December 2002, (n.23). at p.7; National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2003 Internet Fraud Report, 1 January 2003 - 31 December 2003, (n.24) at p.7; National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2004 Internet Fraud - Crime Report , 1 January 2004 – 31 December 2004, (n.25).at p.8; National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2005 Internet Fraud - Crime Report, 1 January 2005 – 31 December 2005, (n.26) at p. 9; National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2006 Internet Fraud - Crime Report, 1 January 2006 – 31 December 2006, (n.27) p.9; National White Collar Crime Center and the Federal Bureau of Investigation, IC3 2007 Internet Fraud - Crime Report, 1 January 2007 – 31 December 2007, (n.28) p.7; National White Collar Crime Center, 2008 Internet Crime Report, (n.29) at p.6; National White Collar Crime Center, 2009 Internet Crime Report, (n.30) at p.18; National White Collar Crime Center, 2010 Internet Crime Report, (n.31) at p.10; National White Collar Crime Center, 2011 Internet Crime Report, 2011 (n.32) at p.11; National White Collar Crime Center, 2012 Internet Crime Report, (n.33) p.17; National White Collar Crime Center, 2013 Internet Crime Report, (n.34) at pp.12-13; National White Collar Crime Center, 2014 Internet Crime Report, (n.35) at pp.10-16.

of a prior cyber law in Nigeria, the EFCC recorded numerous convictions in respect to the aforementioned fraud related acts as part of her role in the enforcement of cybercrime in Nigeria. This is quite obvious from the comprehensive law model. The dilemma here is that there is a total disconnect about the efforts of the EFCC in the literature in terms of her efforts thus far in eradicating cybercrime in Nigeria. This could be borne out of the fact that most convictions recorded thus far by the EFCC are unreported. However, without recourse to the comprehensive law model i.e the positive achievements of the EFCC in the absence of a prior comprehensive law on cybercrime, invariably portrays that the conclusion reached labeling Nigeria as a safe haven for cyber criminality is myopic.

Moreover, it is inexplicable that the United States of America consistently ranked globally as number one between 2002 and 2014 by the Internet Crime Reports is not tagged as the hub of cybercrime and cyber criminality. The reports show a resounding proliferation and perpetration of cybercrime in the United States of America despite being equipped with robust and anti computer crimes and cyber laws and policies i.e Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act(ECPA), National Infrastructure Protection Act, Cyberspace Electronic Security Act, Digital Millennium Copyright Act, Patriot Act of 2001, Cyber Security Enhancement Act (CSEA), Anti-Phishing Act, Cybersecurity Act of 2010, Cyber Security and Internet Freedom Act of 2011, USA Cyber Security Information Sharing Act of 2012, SECURE IT Act of 2012, Cyberspace Policy (Draft), Fraudulent Online Identity Sanctions Act, The Computer Fraud and Abuse Act, Internet Freedom Preservation Act of 2008, Economic Espionage Act (EEA), National Cybersecurity and Critical Infrastructure Protection Act of 2013 (NCCIP), NIST Preliminary Cybersecurity Framework.

The irresistible conclusion that can reached from the foregoing is that a country's lack of a cyber law and/or poor global rating is not

a prerequisite for tagging such a country as a safe haven for cybercrime and cyber criminality. The country's efforts put in place to eradicate the menace of cybercrime should be the primary antidote, as shown from Nigeria's perspective in the comprehensive law model hereafter.

Comprehensive Law Model

This model recognizes the absence of a comprehensive cyber law prior to the enactment of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act 2015, currently the legal framework for investigating and prosecuting cybercrime perpetrators in Nigeria. It however, asserts that despite the obvious absence of a prior comprehensive cyber law, in order to nib in the bud the nefarious activities of cybercrime perpetrators in Nigeria, law enforcement agents relied on the Advance Fee Fraud and Other Fraud Related Offences Act, 2006.

Specifically, the Economic and Financial Crimes Commission was established by the Economic and Financial Crimes Commission (Establishment) Act, 2004 and consequently charged with the responsibility of investigating and prosecuting all economic and financial crimes.[39] An instance of economic crime is provided in section 1 of the Advance Fee and Other Related Fraud Offences Act, 2006 with the EFCC at the helm of affairs to enforce the provisions of the said law.[40]

It is safe to say that the EFCC (Establishment) Act 2004, empowered the EFCC to investigate and prosecute perpetrators of cybercrime while placing reliance on the Advance Fee Fraud and Other Fraud Related Offences Act, 2006. Section 7 (2) of the EFCC (Establishment) Act 2004, equipped the Commission with the responsibility of enforcing the provision of '… (b) The Advance Fee Fraud and Other Fraud Related Offences Act 2006.'[41]

[39] Economic and Financial Crimes (Establishment) Act, 2004, s. 1
[40] Ibid. s. 7(2)
[41] Ibid.

Consequently, prior to the enactment of the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act 2015, the Laws regulating cybercrime in Nigeria includes:- The EFCC (Establishment) Act 2004, the Advance Fee Fraud and Other Related offences Act 2006, the Money Laundering(Prohibition) Act, 2011, Constitution of the Federal Republic of Nigeria, 1999 (as amended) has useful provisions regarding a privacy right which is against illegal computer hacking or online stalking by private or official persons; also the Evidence Act 2011,[42] serves to regulate the activities of cybercrime in Nigeria.

In this regard, the EFCC made tremendous impact in the enforcement of cybercrime perpetration in Nigeria. Typical instances of cybercrime perpetrated in the form of online fraud in Nigeria were; Advance Fee Fraud Scam, Contract Scam, Inheritance or transfer Scam, Romance and Dating Scam, Employment Scam, Identity/Phishing Scam, Charity Scam, Lottery Scam, Crude oil/Mineral Resources sales Scam, Scholarship Scam, Car Auction Sale Scam, Immigrant/Visa Scam etc.

It is unfortunate that despite the notable achievements of the EFCC in cybercrime enforcement in Nigeria, commentators have nicknamed Nigeria as the hub of cybercrime and cybercrime perpetrators. Taiwo A. Oriola, attributed the flourishing nature of cybercrime to lack of effective enforcement hence there has not been a single reported conviction of any of the alleged perpetrators of advance fee fraud schemes in cyberspace from Nigeria. He concluded that the Nigerian Government must show commitment to the eradication of this crime and the best way to do it is to prosecute and make examples of those already arrested.[43] As stated earlier, these assertions are propelled by the lack of literature on the numerous convictions that have been recorded in Nigeria in respect to cybercrime.

[42] Evidence Act 2011. S. 84

[43] Taiwo A. Oriola, (n.5) at 247.

This model acts as gap filling to the literature by showing the numerous convictions recorded thus far by the Nigerian law enforcement agents, EFCC and to justify a radical shift from the head long impression of lack of enforcement of cybercrime in Nigeria prior to the enactment of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015. The convictions herein were recorded in the superior courts of record (i.e High Courts, Federal High Courts, Court of Appeal and Supreme Court) due to the jurisdiction of the court in relation to the trial of cybercrime offenders that is particularly granted to the Federal High Court or the High Court of a State or the High Court of the Federal Capital Territory (FCT) according to the EFCC (establishment) Act 2004 by implication.[44] The Advance Fee Fraud and Other Fraud Related Offences Act 2006 also give the Federal High Court, the State High Court or the High Court of the Federal Capital Territory (FCT)[45] the jurisdiction to try offenders of cybercrime under the Act by implication. Therefore, in Nigeria the jurisdiction to try cybercrime offenders lies with the Federal High Court, the State High Court or the High Court of the Federal Capital Territory (FCT). This situation is bound to change upon the implementation of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 which has solely given the Federal High Court's jurisdiction to entertain cybercrime offences under the Act.

The Nigerian Supreme Court have had course to entertain an online Advance Fee Fraud case; *Mike Amadi vs Federal Republic of Nigeria*[46] where the Appellant(Mike Amadi) was charged before the High Court of Lagos State holden at Ikeja by EFCC *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,

[44] EFCC (Establishment) Act, 2004, s. 19 (1)

[45] The Advance Fee Fraud and other related Offences Act, 2006, s.14.

[46] (2008) 12 SC (pt.III) 55 or 36.2 NSCQR 1127

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.

In *Harrison Odiawa vs Federal Republic of Nigeria*,[47]sometime between March 2003 and 2004 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 Advance 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

[47] (2008) All FWLR (pt.439) 436; (2008) LPELR-CA/L/124/2006

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 lead 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."[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.

Apart from the above recorded convictions by the EFCC at both the Supreme Court and Court of Appeal, based on available data from

[48] (2000) All FWLR (pt.439) 436; (2008) LPELR-CA/L/124/2006 - The accused was also found guilty of the offences of conspiracy, forgery, uttering and in possession of documents containing false pretences. Count 1- 12yrs imprisonment without option of fine and to pay restitution of 10,000.00 Pound Sterling to PWI; Count 2- 12yrs imprisonment without option of fine; Count 8- 12yrs imprisonment without option of fine and to pay PW1 restitution of 195,000.00 US Dollars; Count 9- 12yrs imprisonment without option of fine and to pay PW1 restitution of 300.000.00 US Dollars etc.

the EFCC; at the Federal High Courts and State High Courts, in 2010, the Commission secured 49 convictions, from which 17 convictions were offences relating to cybercrime, online fraud, internet scam etc and it was discovered that internet related scam recorded about 34.7 percent from the total number of convictions secured by the EFCC; In 2011, the Commission secured 67 convictions, from which 38 convictions were cybercrimes, online fraud etc and internet related scam recorded about 56.7 percent of the total number of convictions recorded; In 2012, the Commission secured a total number of 87 cases regarding convictions, from which cybercrime recorded a total number of 49 convictions in court representing about 56.3 percent of the total number of convictions secured by the Commission; In 2013, the Commission secured a total number of 117 convictions in all its cases. From the 117 convictions secured, 33 were from cases of online fraud, Advance fee fraud and internet scam. Therefore, it represented a total number 42.5 percent of the total convictions secured;[49] In 2014, the Commission secured 126 convictions, from which about 59 convictions are in cybercrime; e-mail scam, internet fraud, internet banking fraud, lottery scam, scholarship scam, romance and dating scam, etc. This represents about 46.8 percent of the total number of convictions secured by the Commission.[50]

Statistically, there was 88% increase rate in the number of convictions secured by the EFCC in the fight against cybercrime perpetrators between 2011 and 2014.[51] This shows that the EFCC performed creditably well in its fight against the perpetrators of cybercrime and online fraud cases. The achievement in terms of the numerous convictions recorded by the EFCC and the resolute fight against cybercrime perpetrators is responsible for the downward plunge of the activities and commission of the offence of cybercrime by these cybercriminals in Nigeria.[52] Consequently, it is

---

49 EFCC 2013 Annual Report 16

50 EFCC 2014 Annual Report 17

51 EFCC, 'Landmark Achievements In The Fight Against Economic And Financial Crimes', (2012-2015),p. 4.

52 EFCC 2014 Annual Report, 19.

arguably unjustified and wrong for the domestic and international literature to have labeled Nigeria as the hub of cybercrime and cybercrime perpetration.

Measures Adopted By EFCC In Combating Cybercrime in Nigeria

Realizing the menace of cybercrime and the need to keep the cyberspace safe for the benefit of cyber citizens, the democratic governance of Nigeria through the EFCC at the helm of affairs devised quite a number of measures which yielded positive results towards enforcing cybercrime in Nigeria. This section identifies the *modus operandi* of the EFCC in eradicating cybercrime in Nigeria which yielded numerous convictions in the superior courts of record (i.e Federal High Courts, Court of Appeal and Supreme Court).

Petitions (verbal, written, social media) and Restitution of Victims of Cybercrimes

Generally, the EFCC accepts verbal petitions (which may subsequently be documented); written petitions from the general public who are victims of cybercrime and cybercrime perpetrators giving details of how the crime was perpetuated. Upon receipt of the petition, EFCC in cognizance of her statutory duties proceeds immediately to investigate the veracity or otherwise of the allegations stated in the petition.[53] In course of the investigation, possible invitations, arrests and detentions are employed. At the conclusion of investigation, perpetrators whose allegations against them have been substantiated are charged before the superior courts of record (High Court or Federal High Court) for trial. To enhance the activities of EFCC, five zonal offices across Nigeria were established in addition to Abuja headquarters to oversee prompt investigation and prosecution of cybercrime perpetrators; North East, Gombe; North West, Kano; South East, Enugu; South West, Lagos; South South, Portharcourt.[54]

[53] EFCC 2013 Annual Report, 10; EFCC Act, 2004, s.7(1) & (2)
[54] EFCC 2013 Annual Report, Administrative Information, xi

For instance, to mention but a few, the cases of *Federal Republic of Nigeria vs Babatunde Bolaji Muritala*;[55] *Federal Republic of Nigeria vs Aimuanwehi Friday Osaretin & 2Ors*;[56] *Nwankwo vs Federal Republic of Nigeria*[57] and *Federal Republic of Nigeria vs Isaac Nvene*[58] were received by EFCC through petitions and accused persons were later charged to court and convicted. The EFCC also received a total of 126 petitions on cybercrime offences and it proceeded to investigate the petitions and 96 of the suspected fraudsters were charged to court.[59] These cases include petitions received by all the zonal offices of the Commission, including Abuja.

The restitution of victims of cybercrime during investigations and/or conclusion of trials in court of perpetrators of cybercrime is one measure adopted by EFCC that gave credibility and plus to her quest to eradicate cybercrime in Nigeria. It is a confidence booster for the EFCC in the global community as it showed to the world that the Commission is ready and willing to fight cybercrime at any rate. A sympathetic case of a blind teacher, Mrs. Mary Iheanacho, was deceived and swindled by a gang of fraudster. Upon diligent investigation, the EFCC was able to recover her money from the fraudsters and a cheque was presented to her at the Enugu Zonal Office of the Commission;[60] Jolanta Kasza, a United States Citizen, who is based in New York, was swindled to the tune of $64,000 (Sixty Four Thousand US Dollars) in an online romance and love affair involving one, Ndekwe Jindu. Based on her petition to the EFCC and consequent investigation, the perpetrator was arrested and the sum of $23,886 (Twenty Three Thousand Eight Hundred and Eight Six US Dollars) was recovered for her and a cheque

[55] Unreported, Suit No. FHC/PH/135C/10/2011
[56] Unreported, Suit No. FHC/B/57C/2011
[57] (2003) 4 NWLR (pt. 809) 1
[58] (2005-2010) ECLR 1.
[59] EFCC 2013 Annual Report, 15
[60] Ibid. 10

presented to her at the United States Embassy in Abuja;[61] Margaret Sanders, who lives in Texas, US, was full of praises for the Commission, when the EFCC helped her recover $2,000 (Two Thousand US Dollars) which she had lost to an internet scammer, one Benny Brown**,** from Warri, Delta State.[62]

The Nigeria Courts have also been liberal in awarding to the EFCC orders for recovery and forfeiture of assets from cybercrime proceeds as a means of restitution for cybercrime victims. In *Federal Republic of Nigeria (FRN) vs Benjamin Otoriomuo*[63] a Lagos State High Court convicted the accused for the offence of obtaining by false pretence and internet fraud and sentenced him to six months imprisonment and ordered that the accused pay the sum of $4,016.25 (Four Thousand Sixteen Dollars, Twenty Five Cents) to the victim as restitution. Similarly in *Federal Republic of Nigeria vs Jeje Olaniran*[64] a Lagos State High Court convicted the accused for the offence of cybercrime contrary to Section 6 and 8 (b) of the Advance Fee Fraud and other related offences Act 2006 and sentenced him to one year imprisonment and ordered that he should pay the sum of $22,500.00 US Dollars (Twenty Two Thousand, Five Hundred Dollars) to the victim as restitution. Also a Federal High Court in Port Harcourt in *FRN v Ibiba Jack*[65], Hon. Justice Aikawa R. M while reading the judgment sentenced the accused person to seven years imprisonment without an option of fine for the offence of obtaining money under false pretence and internet fraud and also ordered for the accused to pay the sum of N29, 700,000 (Twenty Nine Million, Seven Hundred Thousand Naira) to two of his victims as restitution. Also, Justice P. I. Ajoku

---

[61] Ibid

[62] Ibid

[63] Suit No. LCD/87C/2013, Judgement delivered on 8 October 2013 (Unreported)

[64] Suit No. LCD/131/2012, Judgement delivered on 21 November 2013 (Unreported)

[65] Suit No. FHC/149C/2007, Judgement delivered on 13 February 2014 (Unreported)

of the Federal High Court Benin in *FRN v Eleoghosa Okhiabor*[66] while sentencing the accused person for the offence of internet scam ordered him to pay the sum of $15,551 (Fifteen Thousand, Five Hundred and Fifty One US Dollars) to his victim as restitution including his sentence of two years imprisonment without an option of fine.

Raids on Cybercafés, Car Shops and Hotels

Legally, operators of telecommunications or internet services or owners of premises being used as a telephone or internet/cyber café are required to register with the EFCC and maintain register of all their customers which is subject to the inspection of authorized officers of the Commission.[67] In order to ensure that all cybercafés in Nigeria are registered and to avoid their use for the perpetration of cybercrime, the Commission carried out series of raids on cybercafés anywhere in the country where it has reasonable suspicion that perpetrators are carrying out their operations without prior information, to ascertain whether or not they are indeed being used by internet scammers. Successful operations lead to arrest of cybercrime perpetrators, seizure of computers, devices as evidence against the suspects. Sometimes, they arrest owners and members of staff of the cybercafés who colluded and for failure to register the cybercafé. These raids are carried out by the Commission in all its zones in the country to curb cybercrime perpetrators[68]. Moreover, the EFCC in collaboration with Association of Cybercafé and Telecommunication Owners in Nigeria (ATCON) banned over night browsing in all cybercafés, mandatory registration for all cybercafé operators, internet service providers (ISP) to be registered with the Commission or risk closure of their

[66] Suit No. FHC/B/25C/2013, Judgement delivered on 24 September 2014 (Unreported)

[67] Advance Fee Fraud & Other Fraud Related Offences Act, 2006, ss.12 & 13; s. 7 of the Cybercrimes Act 2015 have in addition stated that all operators of cybercafé shall register as a business concern with the Computer Professionals' Registration Council.

[68] Interview with Mr. C. A Ajah, staff EFCC policy, planning and strategy Department, Abuja, 25 April 2015

businesses or face the penalties as stipulated in the Act. It mandated the installation of acceptable hardware surveillance systems in the cyber cafe to monitor the activities of the computer users; the architecture of all cybercafés were instructed by the EFCC to be constructed in such a way that all computer systems in the cybercafé should be visible such that none should be concealed from the general public entering the Cybercafé; It further mandated ATCON to inform its members or other cybercafés to subscribe to only registered and licensed ISPs in the country; each cybercafé operator should serve as a watch dog to each other and report any cybercafé violating the provisions of the Act; since they have direct access to the EFCC, they should not delay or fail to make a report.[69] The EFCC also placed discrete surveillance in hotels, and car shops with a view to apprehending suspected internet scammers thereby curbing cybercrime.[70]

Bursting of Homes, Offices and Hideouts of Cybercrime Perpetrators

In recognition of the reduction of patronage of cybercafés by cybercrime perpetrators, due to access to the internet and to the world from the leisure or comfort of their homes or offices through MODEM,[71] made possible by the expansion of Global System for Mobile Communications (GSM). GSM service providers began operating internet service through its GSM to its subscribers, the EFCC made it compulsory through the Nigerian Communication Commissions (NCC) for all GSM providers to register the Subscriber Identity Module (SIM) Cards, so that the Names, Photographs and Finger prints of its internet subscribers would be stored to ease tracing of cybercrime perpetrators after the

---

[69] EFCC Guidelines to Cybercafé Owners in Nigeria 2007.

[70] Interview with Mr. C. A Ajah, staff EFCC policy, planning and strategy Department, Abuja, 25 April 2015.

[71] Ibid

commission of cybercrime.[72] Consequently, cybercrime perpetrators who operate from the comfort of their homes, offices and other hide outs as safe locations for defrauding people are traced through the data and Biometric collected by the Communication Companies. Through covert intelligence, their homes, offices and hide outs in discrete locations were raided by the EFCC which yielded results in helping the EFCC curb the activities of Cybercrime perpetrators who operate from presumed safe locations.[73]

Co-operation with Banks and other Financial Houses

The EFCC in order to curb the activities of cybercrime perpetrators established a synergy with banks and other financial houses to help arrest cybercrime offenders sequel to the provision of the EFCC (Establishment) Act[74] and Money Laundering (Prohibition) Act 2011. The bank and other financial houses are mandated to report lodgments or cash transactions exceeding certain limits[75] for individuals or corporate bodies. This is done through the Suspicious Transaction Report (STR) given to the EFCC by the banks.[76] The Commission also secured the cooperation of the operators of Bureau de change across the country under the foreign currency transaction to report individuals or corporate bodies with excess foreign currency to the Commission.[77]

Stop and Search Operations

The EFCC deviced this method to apprehend suspected internet fraudsters.[78] Where there is a reasonable suspicion by the

---

[72] Ibid

[73] Interview with Mr. C. A Ajah, staff EFCC policy, planning and strategy Department, Abuja, 25 April 2015

[74] EFCC ACT 2004, s.6(a)-(j); See *Federal Republic of Nigeria vs Babatunde Bolaji Muritala*, (supra) where Oceanic Bank reported the accused to EFCC.

[75] N5m for individuals, N10m for corporate bodies

[76] EFCC 2014 Annual Report, 34

[77] Ibid 35

[78] Interview with Mr. C. A Ajah, staff EFCC policy, planning and strategy Department, Abuja, 25 April 2015

Commission's operatives in respect to a vehicle or its occupants as cyber fraudsters, a stop and search operation is embarked upon to search persons in the vehicle, including the vehicle thoroughly.[79] Most times a thorough search on individuals and vehicles reveals that they have links to cybercrime. Consequently, their telephones and lap tops are searched to ascertain the level of their involvement in internet fraud.[80]

Collaboration with Sister Agencies

The EFCC sometimes, collaborate with other Law Enforcement Agencies such as the Nigeria Police, the Nigerian Army, Nigerian Custom, the Nigeria Immigration Service and the Nigerian Security and Civil Defence Corp (NSCDC) to help apprehend suspected internet fraudsters and cybercrime perpetrators.[81] For instance, the case of one Phillips Agbodobiri[82] who was convicted on February 12, 2015, and sentenced to 2 (Two) years imprisonment without an option of fine for offences bothering on false pretences and internet scam[83] was arrested alongside 19 others on January 2013 by men of the Fourth Brigade, "Operation Pulo Shield'' of the Nigeria Army, Benin City and handed over to the EFCC for further investigation and prosecution. In *Fedral Republic of Nigeria vs Jacob Chinenye Isintume*,[84] the accused that was found in possession of documents and laptop used in committing internet fraud against people was apprehended by Lt. B.G Lawal of the Nigerian Army, Bony Camp and transferred to EFCC for investigation. The accused was later found guilty and convicted.

Development of Software and Malware

---

[79] Ibid

[80] Ibid

[81] Ibid

[82] Available at <www.efccnigeria.org> Last accessed 13 March 2015

[83] Contrary to AFF and Other Related Offences Act 2006, S.6 and S.8 (b); punishable under AFF and Other Related Offence Act 2006 s.1(3).

[84] Charge No. FHC/PH/34C/2009, Judgment delivered on 23 March 2012 (Unreported)

To facilitate the investigation of cybercrime, the EFCC launched the "Operation Eagle Claw" in 2008. In this operation, a software that facilitates the sniffing out of fraudulent e-mails called the "Eagle Claw Software" was developed and deployed by the EFCC to apprehend cyber crime perpetrators.[85]

Conclusion

This discourse is set out to examine the assertions in the literature nicknaming Nigeria as the hub of cybercrime and cybercrime perpetration premised on the lack of a prior cyber law and poor global rating of Nigeria. The basis for the conclusion has been examined and consequently successfully argued that the basis is one-sided and have been whittled down by the successes of numerous cybercrime convictions recorded and effective and efficient measures taken by the Nigerian Government through EFCC to eradicate cybercrime in Nigeria through the Myopic or Constitutional and Comprehensive Law Models. It is hoped that the recent Nigerian Cybercrimes (Prohibition, Prevention Etc) Act, 2015 passed by the House of Representatives on 22 April 2015 and the Senate on 23 April 2015, which was signed into law by former President Dr Goodluck Ebele Jonathan on 15 May 2015 would be effectively implemented by the present administration by the provision of a comprehensive cyber security strategy for Nigeria; establishment and maintenance of a National Computer Emergency Response Team(CERT) Co-ordination Center that will be responsible for the management of cyber incidences in Nigeria; establishment of a National Computer Forensic Laboratory; Inauguration of the Cybercrime Advisory Council. This will serve as a morale booster to sustain and increase the prospects of fighting cybercrime perpetrators to a standstill.

---

[85] J.Oates, 'Operation Eagle Claw Net', *Nigerian Spammers,* 2009,18, the A register, available at <http;//www.register.co.uk/2009/10/23/Nigeria_police_success> Last accessed 27 January 2015.