Have we put out Best Foot Forward? An Appraisal of Nigeria's Cybercrime Act (2015) in the Context of Global Realities

Daniel Philemon Saredau,[1]

Abstract

The internet is a phenomenon of unlimited possibilities. The domain of the internet is the cyberspace. Despite its tremendous merits, the cyberspace has been employed by unscrupulous elements to occasion great harm. Cybercrime refers to the unscrupulousness committed in the cyberspace. As a global issue, the United Nations, the African Union, the Council of Europe and the Economic Community of West African States, have designed legal initiatives to prevent and combat cybercrime. The proliferation of internet in Nigeria came with explosion in cybercrime, notably cyber-fraud, popularly referred to as "yahoo-yahoo". The country's notoriety for cyber-fraud is globally established. Before 2015, such laws as the Criminal Code, Penal Code and the Advance Fee Fraud Act were utilised to combat the crime. However, the need for a more potent legislation remained eminent, hence the enactment of the Cybercrime (Prohibition, Prevention etc) Act 2015 ("the Act). This paper is both descriptive and prescriptive. It explores the contents of the Act and annotate as necessary. It also assesses the Act in the light of global efforts directed at combating cyber-criminality. The article concludes by identifying key points of the Act, exposing some shortcomings of the Act and proffering recommendations for review and in implementation of the Act. The key finding of the article is that although there are shortcomings requiring improvement, the Act is currently Nigeria's best foot forward in the fight against cyber-criminality. Therefore, all stakeholders must work in concert to ensure its success.

Keywords: Cybercrime, Nigeria Cybercrime Act, Internet.

[1] Daniel Philemon Saredau, LLB, LLM (Ibadan) BL;
Lecturer, Faculty of Law, Taraba State University; dansaredau@yahoo.com; 08067713610

1. Introduction

In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet... By the year 2020, the number of networked devices (the 'internet of things') will outnumber people by six to one, transforming current conceptions of the internet. In the hyper-connected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity.[2]

We live in a cyber-age where almost everything is connected into a virtual network. Time seamlessly meets with space. Everything becomes instantaneous as innovations take place apace. One can hardly keep up with the pace. These innovations entail transformations in our transportation, communication, commercial, media, security, etc., systems. The cyberspace is the virtual global domain where all these activities take place.

To protect the cyberspace and ensure its orderly operation, law as regulator of all human activities, must keep pace with technology. This is so because despite its huge positive impacts, the cyber regime can be, and has been, adapted by unscrupulous elements to occasion tremendous mischief. There is, therefore, no gainsaying that the cyberspace has become toxic. The Janus-faced or oxymoronic nature of the internet makes it easily adaptable for doing as much bad as the good it is envisioned for. To this end, the right legal framework must be created to sieve out its negative impacts. Cyber capacity, to be beneficial, must be matched with cyber security.[3] This is where cybercrime legislations come into play. Rudimentarily, therefore, cybercrime legislations proscribe unacceptable cyber behavior and label them as crimes with appropriate penalties tagged to them.

---

[2]United Nations Office on Drugs and Crimes, 2013.*UNODC Comprehensive Study on Cybercrime- Draft.* Page xvii

[3]Moses-Oke, R.O., 2012. Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT*). Journal of Philosophy, Science & Law 12.* Retrieved Feb., 27, 2018 from http://jpsl.org/srchives/cyber-capacity-without-cyber-security-case-study-of-nigerias-national-policy-information-technology-npfit

The advent of the internet has greatly improved the quality of human life in today's global world, not least in Nigeria.[4] Steadily, but surely, from its humble beginnings in 1996, the internet phenomenon has blossomed in Nigeria. According to data from the International Telecommunications Union, usage of internet in Nigeria, which was 0% in 1996, rose to 0.3% in 2000, then 1.5% by 2004, 7% by 2007 and 15.9% by 2008.[5] Prior to 2001, the cyber fraud trend was not globally associated with Nigeria and advocacy for Nigerian cybercrime legislation was not prevalent.[6] From then, however, many Nigerian internet users employed the internet for fraudulent and other criminal activities such that Nigeria became renowned for internet related crimes.[7] In 2001, the American National Fraud Information Centre reported that Nigeria has the fastest growing online scam.[8] That report was indeed prophetic as there was such an upsurge of cyber fraud and other cyber crimes in Nigeria culminating in the country's ascendancy to the number three spot in the worldwide cybercrime trends index by 2010.[9] Today, Nigeria's notoriety for cyber crime is well established. This notoriety comes with

---

[4]Akomolade, T.I, 2008. Contemporary Legal Issues In Electronic Commerce in Nigeria. *Potchefstroomse Electronic Law Journal* 11.3:1-24. Retrieved March 20, 2018 from http://www.ajol.info/index.php/pelj/article/view/42234

[5] Vanguard Newspapers, October 27, 2010. Internet: 13 years of growth in Nigeria. *Vanguard News*. Retrieved March 30, 2016 from http://www.vanguardngr.com/2010/10/internet-13-years-f-growth-from-ground-zero-in-nigeria-from-1960-1996/

[6]Frank, I & Odunayo, E, 2013.Approach to Cyber security issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education 1.1*: Retrieved March 18, 2018, from http://ijcrsee.com/index.php/ijcrsee/article/view/11/114

[7] Moses-Oke, R.O., 2012, *op.cit*

[8] Ihenyen, S.I, August 13, 2015. Cleaning up Nigeria's Cyberspace- New Cybercrime Act to the rescue.*Nigerian Law Today*. Retrieved March 16, 2018 from http://www.nigerianlawtoday.com/2015/08/cleaning-up-nigerias-cyberspace-new.html

[9]Nkereuwem, E., December 1, 2010. *Nigeria comes 3rd in global cybercrimes survey*. Retrieved March 2, 2018 from http://www.abujacity.com/abuja_and_beyond/2010/11/nigeria-comes-3rd-in-global-cybercrimes-survey-.html

huge financial losses to the country- it is reported that Nigeria losses N90 billion to cybercrimes annually.[10]

The foregoing actuated an urgent need for the country to, at an institutional level, understand the internet phenomenon and to curb its ill effects. The government therefore, commissioned a body of experts to design a National Policy on Information Technology 2001. Ordinarily, such policy should have offered the much needed understanding for the prevention and eradication of criminal activities in cyberspace but regrettably, it focused only on the projected possible benefits of Information Communication Technology (ICT), without being critically sensitive to the possibility of ICT abuse.[11] In effect, the policy portrayed the government as lacking sufficient commitment to deal with the problem of cyber-criminality in the country.[12]

Thankfully, with the enactment of the *Cybercrime (Prohibition, Prevention etc) Act 2015*,[13] Nigeria has now gone passed the inadequacies of the yesteryears. The Act traces its origin to the Federal Government's cybercrime working group, called the Nigeria Cybercrime Working Group (NCWG) which was launched in 2004.[14] The NCWG produced the National Cybercrime Initiative (NCI) saddled with the task of identifying and outlining appropriate legal and institutional framework for securing computer systems and networks, and for protecting critical infrastructure in Nigeria. The initial draft of the Cybercrime Bill, sponsored by the NCWG was proposed to the National Assembly in 2004**.** However, the bill lagged in the National Assembly until November 2011 when the Office of the National Security Adviser (ONSA) harmonized the Bill

---

[10]Ajijola, A., March 31, 2016. Nigeria loses N90bn to cybercrimes annually- NITDA Consultant. *The Punch Newspapers*. Retrieved March 31, 2018 from http://www.punchng.com/nigeria-loses-n90bn-to-cybercrimes-annually-nitda-consultant/

[11]Moses-Oke, R.O., 2012.*Op cit.*

[12] ibid

[13] Hereinafter simply referred to as "the Act"

[14]Ezeoha, A.E., 2006. Regulating Internet Banking in Nigeria: Some Success Prescriptions – Part 2. *Journal of Internet Banking and Commerce, 11:23*. Retrieved Feb., 13, 2018 from http://www.arraydev.com/commerce/JIBC/2006-04/Nigeria-2_F.asp

with other miscellaneous bills relating to cyber security into the Cybersecurity Bill, 2011.[15] Four years later, and with the added vigorous efforts of other advocates, the Act was finally enacted and signed into law by former President Goodluck Jonathan in May, 2015. The Act provides the much needed but long elusive legal framework for effective tackling of cybercrime in Nigeria.

This paper is both descriptive and prescriptive. It explores the contents of the Act and annotate as necessary. It also assesses the Act in the light of global efforts directed at combating cyber-criminality. The article concludes identifying key points of the Act, exposing some shortcomings of the Act and proffering recommendations for review and in implementation of the Act.

2. Annotation of the Act

The Act, structured into eight parts and two schedules, has a total of 59 sections.

2.1 Part I- Object and Application

Section 1 of the Act rehashes its explanatory memorandum. It identifies the three broad objectives of the Act, to wit:

a. providing effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
b. ensuring the protection of critical national information infrastructure (CNII); and
c. promoting cyber-security and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

By *section 2*, the Act applies throughout Nigeria.

---

[15]Lambo J., &Oghenochukwu G., 2014.Cybersecurity Bill 2013- ray of hope or poisoned chalice? *Newsletter- International Law Office.* Retrieved March 21, 2018 from http://internationallawoffice.com/Newsletter/IT-Internet/Nigeria/Udo-Udoma-Belo-Osagie/Cybersecurity-Bill-2013-ray-of-hope-or-poisoned-chaliceThe ONSA went further, in the context of the overall national security, and came up with two other cyber-security documents: Nigeria's National Cyber-security Policy and National Cyber-security Strategy.

2.2 Part II- Protection of CNII

Part II, concerned with achieving the second objective of the Act as identified above, grants the President powers to, on the recommendation of the National Security Adviser (NSA), issue Orders designating certain computer systems, and/or networks, whether physical or virtual, and/or computer programs, computer data and/or traffic data vital[16] to Nigeria as constituting CNII.[17] Such Presidential Orders may prescribe rules for the adequate protection, management and control of data and other resources in any of such CNII.[18] The Order may also require the ONSA to audit and inspect any CNII at any time to ensure compliance with the provisions of the Act.[19]

2.3 Part III- Offences and Penalties

In line with its first objective identified above, Part II of the Act proscribes certain inimical cyber conducts, labels them as offences with stipulated penalties.

i. OFFENCES AGAINST CNII: *Section 5* provides that a person, who commits any offence against any designated CNII is liable to be imprisoned for up to 10 years without option of fine. This section does not create a stand-alone offence but further criminalises an offender whose offence is committed against any designated CNII.[20] Heavier sentences are provided where the offence results in grievous bodily harm (15 years) or death (imprisonment for life).

---

[16] What makes them vital? They are deemed vital because their incapacitation or destruction or interference would have debilitating impact on security, national or economic security, or national public health and safety.

[17] Section 3 (1)

[18] Section 3(2)

[19] Section 4

[20] As at the time of this article, the writer is unaware of any such designation. To that extent, it is safe to say that at present, no offence can be committed under section 5.

ii. UNLAWFUL ACCESS TO COMPUTER: *Section 6 (1)* relates to obtainment of data vital to national security. The offence is committed when a person without authorisation and with the necessary mens rea of intent,[21] accesses a computer system or network for fraudulent purposes to obtain data vital to national security. The penalty is imprisonment of up to5 years or fine of up to N5 million or both. Under *Section 6(2),* if the offender obtains computer data,[22] secures access to any program,[23] commercial or industrial secrets or classified information, the punishment is upped to 7 years imprisonment or N7million fine or both. If the offender uses a device[24] to avoid detection or attribution to the offences aforementioned, that itself is an offence punishable with imprisonment of up to 7 years or N7million fine or both. Trafficking[25] in passwords or other codes for gaining unlawful access to a computer[26] is also criminalised as an offence

[21] Most of the offences created under the Act require intent as mens rea.
[22] By Section 58 "computer data" include "every information including information required by the computer to be able to operate, run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the program the computer user is running"
[23] By Section 58 "Computer program" or "program" means "a set of instructions written to perform or execute a specified task with a computer"
[24] By Section 58 "device" means "any object or equipment that has been designed to do a particular job or whose mechanical or electrical workings are controlled or monitored by a microprocessor"
[25] By Section 58 "Traffic" means "to sell, transfer, distribute, dispense, or otherwise dispose of property or to buy, receive, possess, obtain control of, or use property with the intent to sell, transfer, distribute, dispense, or otherwise dispose of such property"
[26]By Section 58 "Computer" means "an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility. All communication devices that can directly interface with a computer through communication protocols shall form part of this definition. This definition excludes the following; portable hand-held calculator typewriters and typesetters or other similar devices"

punishable with 3 years imprisonment or N7million fine or both.

iii. REGISTRATION OF CYBERCAFÉ: Under *section 7*, all operators of cybercafés are to register as business concerns with the Computer Professional's Registration Council[27] in addition to a business name registration with the Corporate Affairs Commission. They shall then maintain a sign-in register of users which register is to be made available to law enforcement officers whenever needed.[28]A person who perpetuates electronic fraud or online fraud using a cybercafé is to be punished with imprisonment for 3years or a fine N1million or both.[29]If connivance by cybercafé owner is established, such owner is liable to be fined N2million or imprisoned for 3 years or both.[30]

iv. SYSTEM INTERFERENCE: Interference with the functioning of a computer system is criminalised by *section 8* and an offender is liable to imprisonment of up to 2years or 5 million fine or both

v. INTERCEPTION OF ELECTRONIC MESSAGES: Interception[31]of electronic messages or other

---

[27] The Computer Professional's Registration Council of Nigeria (CPN) is a body corporate charged with the control and supervision of the computing profession in Nigeria. It was established by Decree No.49 of 1993. Its website is at http://www.cpn.gov.ng

[28] This is a vital provision that would help cybercafés keep track of their customers and, a fortiori, the law enforcement agents to easily track down persons who employ cyber cafes to commit offences under the Act

[29]cf Section 14. It seems in section 7(2), the important ingredient is the use of a cybercafé, hence a person who commits electronic fraud but not in a cybercafé is not liable under section 7(2) but section 14.

[30] Section 7(3) Section 7 (4).It is arguable that factors such as failure of the operator to register or to keep a sign-in register as required may show connivance by omission to satisfy section 7 (4).

[31] Interception is defined by section 58 as "in relation to a function of a computer system or communications network, includes listening to or recording of communication data of a computer or acquiring the substance,

processes through which money or other valuable information is being conveyed is criminalised by *section 9.* An offender is liable to imprisonment for up to 7 years in the first instance and 14 years on second conviction. Under the Act, this is the only section providing for a higher punishment for a repeat offender. It must be stressed that this section only concerns itself with electronic messages through which money or other valuable information is conveyed. Hence, interference with electronic messages that do not convey money or valuable information is not criminalised hereunder. The construction of what constitutes "valuable information", therefore, becomes crucial. Regrettably, the Act did not define the term and hence, the question remains moot.

vi. TAMPERING WITH CRITICAL INFRASTRUCTURE: Under *section 10,* an employee exposed to critical infrastructure who uses same in an unauthorised way or who intentionally permits or tampers with same commits an offence punishable withN2millionfine or 3years imprisonment.

vii. WILFUL MISDIRECTION OF ELECTRONIC MESSAGES: *Section 11* criminalises any person who willfully misdirects electronic messages with either the intention of fraudulently obtaining financial gain as a result thereof or defeating the essence of such message. The punishment herein is 3 years imprisonment or N1million fine.

viii. UNLAWFUL INTERCEPTIONS: *Section 12(1)* criminalises the intentional and unauthorised interception by technical means of a non-public transmission of computer data, content or traffic

---

meaning or purport of such and any acts capable of blocking or preventing any of these functions;"

data. An offender is liable to 2 years imprisonment or fine of N5 million or both.

Section 12(3) criminalises an employee who intentionally hides or detains electronic messages, electronic payments, credit and debit card found by or delivered to him in error and which to his knowledge ought to be delivered to another person. The punishment is imprisonment for 1 year or fine of N250, 000 or both.

ix. COMPUTER RELATED FORGERY: Knowingly altering computer data to make it inauthentic with intention that such inauthentic data may be considered or acted upon as authentic is criminalised by *section 13*. It does not matter whether or not the data is readable or intelligible. The punishment is imprisonment of not less than 3 years or fine of not less than N7million or both.

x. COMPUTER RELATED FRAUD: *Section 14 (1)* makes it a criminal offence for a person with knowledge but without authorization to use or manipulate computer data so as to cause loss of property to another. Liability herein does not depend on whether or not economic benefit is conferred to oneself or another person but it suffices if loss is caused to property of another. The punishment is imprisonment for minimum of 3 years or fine of minimum of N7million.

Section 14(2) penalizes the use of electronic message to fraudulently misrepresent facts causing damages or loss by imprisonment of minimum 5 years or fine of minimum N10million or both. This provision takes care of the so-called “yahoo-yahoo” boys who initiate fraudulent electronic messages to dupe others. It is instructive that the penalty herein is specified in the minimum.

xi. THEFT OF ELECTRONIC DEVICES: Theft of Automated Teller Machine (ATM) is punishable by

imprisonment of up to 7 years or fine of up to N10million or both. Additionally, all proceeds of the theft are to be forfeited to the lawful owners of the ATM. An attempt to steal an ATM is penalized by imprisonment of up to 1 year or fine of up to N1million or both. In this age where financial institutions employ alternative channels to ease the stress of transactions by their customers, the provisions of *section 15* is very germane as it protects these alternative channel devices chiefly ATMs, Point of Sale (POS) and other card acceptor devices from thieves.

xii. UNAUTHORIZED MODIFICATION OF COMPUTER SYSTEMS, NETWORK DATA AND SYSTEM INTERFERENCE: The intentional and unauthorised modification[32] of data in any computer system or network is punishable by imprisonment of up to 3 years or fine of up to N7million or both. By *section 16(3)*, an intentional and unauthorised act which causes the serious hindering of the functionality of computer system is punishable by imprisonment of up to 2 years or fine of up to N5 million or both.

xiii. ELECTRONIC SIGNATURES: By *section 17 (1) (a)*, electronic signatures in respect of purchases of goods and other transactions are binding. In addition to *section 93 of the Evidence Act, 2011*, this provision has laid to rest the nagging contentions about the legal effect of electronic signatures under the Nigerian law. The burden of proving authenticity of such signature lies on the person who contends.[33] He who asserts should prove.[34]

---

[32] By section 58, "Modification" means "deletion, deterioration, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any means"

[33] Section 17(1)(b)

[34] Section 131 Evidence Act, 2011

Section 17(1)(c) penalizes any person who, intending to defraud or misrepresent, forges through electronic devices, another person's signature or company mandate with imprisonment of up to 7 years or fine of up to N10 million or both.[35]

Section 17(2) excludes some transactions from the categories of contractual transactions or declarations that are valid by virtue of electronic signature:[36]

a.) testamentary dispositions such as wills and codicils;
b.) birth and death certificates;
c.) family law related issues such as marriage, divorce and adoption;
d.) court or judicial related processes, documents or instruments such as court orders, notices, affidavits, pleadings and motions
e.) cancellations or terminations of utility services
f.) any instrument required to accompany transportation or handling of dangerous materials either solid or liquid in nature;
g). any document ordering withdrawal of drugs, chemicals and any other material either on ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.

xiv. CYBER TERRORISM: In this age of global terrorism, there is no length terrorists would not go to achieve their nefarious aims. The immense potentials of the cyberspace have, therefore, been employed by terrorist elements to perpetrate their

[35] Section 17(1)(c)

[36] Electronic signatures in respect of the specified transactions or declarations are, therefore, of no legal validity. Perfunctorily, this provision may be in conflict with section 93 of the Evidence Act, 2011. However on deeper look, it stands to reason that while the Act is only concerned with the legal validity or bindngness of the transaction in question, the Evidence Act is concerned with whether such documents can at all be admitted in evidence as proof of the fact that there was such signature, albeit, invalid.

dastardly acts. *Section 18* criminalises the use of computer or computer system or network for the purposes of terrorism and punishes a person convicted of cyber terrorism with life imprisonment. The sentence definitely fits the crime in view of the horrendous effects of terrorism.

Subsection 2 refers us to the *Terrorism (Prevention) Act, 2011, as amended* for the definition of what constitutes *"terrorism"*. Under the *Terrorism (Prevention) Act, 2001, as amended*, the definition of "*terrorism*" is tricky and quite frankly, can be adopted to label a wide miscellany of criminal activities as terrorist acts.

xv. POSTING AND AUTHORIZING ACCESS: *Section 19* imposes a duty on financial institutions to put in place effective counter-fraud measures to safeguard their sensitive information.

xvi. FRAUDULENT ISSUANCE OF E-INSTRUCTION: An employee of a financial institution charged with e-transactions, who issues false electronic or verbal messages with intent to defraud, is guilty of an offence under *section 20* and liable to imprisonment for up to 7 years.

xvii. REPORTING OF CYBER THREATS: *Section 21* imposes a duty on all operators of computer system or network whether public or private to immediately inform the National Computer Emergency Response Team Coordination Centre (ngCERT) of any cyber threats. An operator who fails to make such report within 7days is liable to be penalized with denial of internet services and additionally, a fine of up to N2 million payable into the National Cyber Security Fund. This provision is a proactive one which ensures communal efforts to expose cyber threats before they fester. However, three questions may be posed: a) what constitutes cyber threat in the context of *section 21*; b) where is ngCERT located and; c) how can ngCERT be contacted?

xviii. IDENTITY THEFT AND IMPERSONATION: *Section 22* criminalises the practice whereby a person engaged by a financial institution employs his special knowledge to commit identity theft of its employer, staff, service provider and consultants with intent to defraud. The punishment is imprisonment for up to 7 years or fine of up to N5million or both.[37] A fraudulent or dishonest use of electronic signature or any other unique identification feature of another person or a fraudulent impersonation of another entity or person, living or dead with intent to generally, confer an advantage to oneself or another or cause a disadvantage to another is also criminalised by *section 22.* Persons, who take up identities of others online, such as, registering on social media (like Twitter or Facebook) with names and profiles of other persons, can be prosecuted under this provision. The punishment is imprisonment for up 5 years or fine of up to N 7 million.

xix. CHILD PORNOGRAPHY AND RELATED OFFENCES: Using a computer system or network to produce child pornography, offer or make available child pornography, distribute or transmit child pornography is a criminal offence attracting imprisonment of up to 10 years or fine of up to N20million or both. Also, intentionally using any computer system or network to procure child pornography or merely possessing child pornography in computer system or computer-data storage medium is also criminalised. The punishment is imprisonment for up to 5years or fine of up to N10million.

By *section 23(2)* knowingly making or sending other pornographic images to another computer by way of unsolicited distribution are penalized with

[37] Section 22 (1)

imprisonment for up to 1 year or fine of up to N250, 000 or both. *Section 23(3)* criminalizes the act of intentionally proposing, grooming, and soliciting a meet with a child through a computer system or network for the purposes of sexual activities. *Section 23(4)* defines child pornography to include pornographic materials that visually depicts a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a minor engaged in sexually explicit conduct. Hence, whether actual or non-actual, a realistic depiction of child pornography is proscribed. *Section 23(5)* defines a "minor" or "child" as a person below 18 years of age.

xx. CYBER STALKING: *Section 24 (1)* criminalises the act of knowingly or intentionally sending or causing to be sent, a message or other matter by computer system or network that is either grossly offensive, pornographic or of an indecent, obscene or menacing character OR that is known to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another person.[38] The punishment is imprisonment for up to 3 years or fine of up to N 7 million or both.

Section 24(2) goes further to criminalize the use of computer system or network for bullying, harassment and threats, especially where such places another in fear of death, violence, bodily harm, apprehension of kidnap, harm to reputation or property. Under *section 24(3),* a court dealing with an offender under this section may further make orders safeguarding the victims from future cyber-stalking. The court can also make an interim order for the protection of victims from further exposure

[38] Section 24 (1)

to alleged offences.[39] These are commendable provisions.

xxi. CYBER-SQUATTING: *Section 25 (1)* criminalises cyber-squatting. It prohibits any person from intentionally taking or using a name, business name, trade mark, domain name or other word or phrase registered or in use by any individual, corporate body or government in Nigeria on the internet without authority or right and for the purpose of interfering with their use by the owner, registrant or legitimate prior user. The offence attracts imprisonment of up to 2 years or fine of up to N 5million or both.

xxii. RACIST AND XENOPHOBIC OFFENCES: Due largely to its anonymity appeal, the cyberspace has become a haven for racists and xenophobes to perpetrate their acts while concealing themselves. To stem this tide, the Act in *section 26* criminalises the distribution or otherwise making available of xenophobic or racist materials[40] to the public through the use of computer systems or networks.
It also criminalises persons who use computer systems or networks to issue threats or insults based on race, tribe, religion, colour, descent and national or ethnic origin. For a country like Nigeria which is still struggling with unity issues and the angst of the civil war, this provision is very apt.[41] However, there is a fine line that should always be made between this provision and the constitutional right to

---

[39]Section 24(5)

[40]cf "pornographic images" as used in *section 23(2).* This validates our argument that "images" is more restrictive than "materials".

[41] On social media and online platforms (such as Facebook, Twitter, Nairaland site) as well in the comment sections of media sites (such as online newspapers), one is usually appalled at the level of insults and threats exchanged between Nigerians based on ethnic and religious grounds. This provision should stem such tide.

free speech. Free speech should and must never be stifled in a free, democratic world.

xxiii. ATTEMPT, CONSPIRACY, AIDING AND ABETTING: A person who attempts to commit an offence under the Act or who aids, abets, conspires, counsels or procures another person to commit any offence under the Act himself commits an offence and is liable to same punishment as the offender.[42]

xxiv. IMPORTATION AND FABRICATION OF E-TOOLS: *Section 28 (1)* criminalizes the importation or fabrication by whatever means of tools, or devices, data, codes that can be used or adapted for use to commit any offence under the Act. By *section 28(2),* mere possession of such devices, data or codes as aforementioned is an offence once it can be shown that the possessor has intention of committing an offence under the Act. Under *section 28(3),* the intentional and unauthorized disclosure of codes for unlawful purpose or gain is criminalized.

xxv. BREACH OF CONFIDENCE BY SERVICE PROVIDERS: Herein, it is criminal for a computer based service provider[43] intending to defraud, to forge or illegally use the security codes of its consumers so as to gain economic advantage.[44] If the offender is a natural person, the punishment is imprisonment for up to 7 years or fine of up to N 5 million or both.[45] But, if the offender is an artificial person, the punishment is that the body corporate is liable to a fine of N 5 million, forfeiture of monetary

[42] Section 27(1)
[43] By section 58, "Service provider" means- (i) any public or private entity that provides to users of its services, the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service"
[44] Section 29(1)
[45] Section 29(2)(c)

value of loss[46] and -if connivance or instigation by principal officers of the body corporate is proved-[47] the court may order its winding-up and direct that all its assets and properties be forfeited to the Federal Government.[48] This provision expands the grounds for winding up a company under *section 408 of the Companies and Allied Matters Act.* Also, by *subsection 2(a),* the veil of incorporation may be lifted so as to discover the human persons behind the breach of confidence and to punish them also.[49] However, such persons may be excused if they can show they are blameless and that they acted *bona fide*.[50]

xxvi. MANIPULATIONS OF ATM/POS TERMINALS: By *section 30(1),* persons who manipulate ATM/POS terminals with intent to defraud are liable to be punished for up to 5 years or fined up to N5million or both. An employee of a financial institution who connives with another person(s) to perpetrate fraud using ATM or POS is liable to be punished with imprisonment for 7 years without an option of fine.[51] The lack of option of fine herein indicates that the legislators deem this offence as very serious.

xxvii. EMPLOYEES RESPONSIBILITY TO HANDOVER ACCESS CODES: Notwithstanding any contractual agreement between employees and their employers, an employee in public or private employment is obligated to handover all access

---

[46] Section 29 (1)
[47] Section 29 (2)(a)
[48] Section 29 (2)(b)
[49] This is an exception to the doctrine of corporation in company law as long established in the case of *Salomon vs Salomon* (1897) A.C 22 HL. There are many other exceptions to the doctrine. See for example, sections 93, 505, 506 and 548 of the Companies and Allied Matters Act.
[50] Section 29(3)
[51] Section 30 (2)

codes to his employer once his contract is terminated.[52] The presumption where he fails to do so is that he wishes to hold his employer to ransom. This offence is punishable by 3 years imprisonment or fine of N3million or both.

xxviii. PHISHING, SPAMMING AND SPREADING OF COMPUTER VIRUS: "*Phishing"* means the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e- mails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user.[53] "*Spamming*" is an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations.[54]A *computer virus* is a computer program which attaches itself to executable system software such as an application program from where it activates and causes severe hindrance of the normal functioning of the computer as well as damages to the computer system or files. *Section 32* provides that the punishment for engaging in phishing, spamming or spreading computer virus is imprisonment for up to 3 years or fine of up to N 1 million.

xxix. ELECTRONIC CARDS RELATED FRAUD: *Section 33* criminalizes a miscellany of fraudulent acts that relate to access devices.[55] In *subsection 1*, a

[52] Section 31
[53] Section 58
[54] ibid
[55] Such as debit cards, credit cards, passwords and Personal identification number.

fraudulent use of access devices to obtain cash, credit, goods or service is a criminal offence attracting imprisonment of up to 7 years or fine of up to N 5 million or both. Additionally, the monetary value of the loss sustained by the owner of the card shall be paid by the offender. By *subsection 2*, the use of a counterfeit or unathorised access device or an access device belonging to another person which use results in loss or gain is an offence punishable by imprisonment of up to 7 years or fine of up to N5 million or both. *Subsection 3* criminalises the stealing of an electronic card. *Subsection 4* creates the offence of dishonestly receiving and retaining a card[56] with intention to use, sell or traffic it to a third party. Under *subsection 5*, a person who with fraudulent intent obtains control over a card as security for a debt commits an offence. The penalty for the offences created in *subsections 3, 4 and 5* is imprisonment for up to 3 years or fine of up to N 1 million. The offender shall also make good the monetary value of any loss sustained by the card holder or forfeit assets acquired with funds from the use of the card.

xxx. DEALING IN CARD OF ANOTHER: Essentially, *section 34* criminalises the receiving and retention of cards of other persons under circumstances which constitute card theft. An offender, on summary conviction, is liable to 3 years imprisonment or fine of N 1 million and shall also repay the monetary value of the loss sustained by cardholder or forfeit proprietary interests in assets or goods acquired with the card.

xxxi. BUYING AND SELLING OF CARD OF ANOTHER: The selling or buying of a card of another person is a criminal offence under *section*

[56] By section 58 *"*Card" means a bank card, credit card, or payment card

35. The punishment is same as dealing in card of another under *section 34*.

2.4 PART IV: DUTIES OF FINANCIAL INSTITUTIONS AND SERVICE PROVIDERS

Today, the cyber-space has become domain for all manners of business transactions. With the huge amount of money involved in these transactions, it is imperative that some safeguards be put in place to prevent fraud and loss. It is in this spirit that part IV of the Act imposes some duties on financial institutions and service providers.

Under *section 37 (1),* financial institutions are obligated to:

a. verify the identity of their customers who require electronic devices such as ATM cards before issuing out such devices;
b. apply the principle of Know Your Customer (KYC) in customer documentation prior to executing electronic transfer, payment, debit and issuance orders.

The failure of a financial institution to obtain proper identity of its customer before executing customer electronic instructions is an offence attracting a fine of N 5 million.[57]Additionally, under *section 37(3),* any financial institution that makes an unauthorised debit on a customer's account is obligated on request to either explain the debit or reverse same within 72 hours. A fine of N 5 million and restitution is provided as penalty for breach of this duty.

On the part of service providers,[58] they are required by *section 38(1)* to keep all traffic data and subscriber information[59]as may be prescribed by the relevant authority responsible for regulation of communication services in

[57] Section 37(2)

[58] By section 58 "Service provider" means - "(i) any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;"

[59] For example GSM service providers are required by the Nigeria Communications Commission (NCC) to keep SIM card Registration information.

Nigeria,[60] for a period of 2 years. The service provider shall, when requested by the communication regulatory authority or law enforcement agency,[61] preserve, hold or retain data or information or release any information so kept. The retaining, retrieval or processing of data if requested by any law enforcement agency shall only be for legitimate purposes as provided under the Act, any other legislation, regulation or by a court order. Confidentiality of data and constitutional right to privacy in relation to the duty of service provider is provided for in *section 38(5).* Contravention of the provisions of *section 38* is an offence attracting imprisonment of up to 3 years or fine of up to N 7 million.

Under *section 39,* a judge may, if satisfied that there are reasonable grounds to suspect that the content of any electronic communication[62] is required for purposes related to criminal investigation or proceedings:

a. order a service provider to employ technical means to intercept, collect, record, or assist competent authorities with the collections or recording of content data and/or traffic;
b. authorise law enforcement agent to employ technical means to collect or record such data.

There is an obvious conflict between this provision and the fundamental right to privacy of citizens.[63] There is no similar provision as *section 38(5).* However, the argument is that national security trumps individual rights. This is still a moot point. In any case, it is safe to say that the judge's discretion to grant order only based on information on oath which adduces very cogent grounds is some safeguard.

Section 40 provides a general duty on service providers to render all necessary assistance to law enforcement agents in

---

[60] At present, that is the NCC pursuant to Nigerian Communications, 2003 Act, CAP N97, LFN 2004

[61] Such as the Department of State Security (DSS), the Economic and Financial Crimes Commission (EFCC) or the Nigeria Police Force (NPF)

[62] Such as short message service (SMS), e-mail, voice mails, multimedia message service (MMS)

[63] Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended)

all inquiries or proceedings under the Act. Such assistance revolves basically around the identification, apprehension and prosecution of offenders as well as the identification, tracking and tracing of proceeds or property, equipment, device related to any offence. Failure of the service provider to perform this duty is an offence attracting a fine of up to N10 million.

2.5 PART V-ADMINISTRATION AND ENFORCEMENT

The administration and enforcement of the Act is conceived as a shared responsibility among the ONSA, the Attorney General of the Federation (AGF), the Cybercrime Advisory Council (Council) and other law enforcement agencies. The ONSA is the coordinating body for all security and enforcement agencies under the Act.[64] It has the role of, amongst others: providing support to all relevant agencies towards the prevention and combating of cybercrimes in Nigeria; establishing and maintaining a National Computer Forensic Laboratory for use of the agencies; building capacity for the effective discharge of their duties by these agencies; ensuring formulation and effective implementation of the cyber-security policy and cyber security strategy;[65] establishing and maintaining a ngCERT for the management of cyber incidences and; coordinating Nigeria's international cyber security cooperation.

The AGF superintends the enforcement of the provisions of the Act.[66] Amongst others, he ensures effective prosecution of cybercrimes and maintains international cooperation with respect to cybercrime and Cybersecurity matters. By *Section 41(3),* all law enforcement, security and intelligence agencies are to develop requisite institutional and manpower capacity for the effective implementation of the provisions of the Act. The Council, which is comprised of the members listed in the *First Schedule,* is established under *section 42* to be headed by the NSA. The Council is mandated by *section 43* to amongst others, formulate and provide general

[64] Section 41 (1)
[65] The National Cyber Security Policy and The National Cyber Security Strategy were published by the ONSA in December 2014.
[66] Section 41(2)

policy guidelines for the implementation of the provisions of the Act and to advice on measures to prevent and combat cybercrimes.

Section 44 establishes a National Cyber Security Fund (the Fund), domiciled in the Central Bank of Nigeria, into which shall be paid and credited monies from miscellaneous sources.[67] Up to 40% of the Fund may be allocated for Counter Violent Extremism related programs. The ONSA is charged with keeping proper records of the Fund. The Fund is to be audited in accordance with guidelines of the Auditor General of the Federation.

2.6 PART VI- ARREST, SEARCH, SEIZURE AND PROSECUTION

A law enforcement officer who requires electronic evidence in relation to crime investigation may apply exparte to a judge in chambers for the issuance of a warrant for that purpose.[68]Additionally, under *section 45(2)* a judge may issue a warrant which authorizes a law enforcement officer to do a number of things, such as: enter and search premises, place or conveyance in relation to criminal investigation; seize, remove and detain anything which contains evidence; use or cause to be used a computer or any device for evidence; use any technology to decode or decrypt data. The warrant is to be granted strictly for the purposes of prevention of crime and other crime investigation related matters. Obstructing a law enforcement officer in the course of his duties or refusal to cooperate with him is an offence attracting imprisonment of 2 years or fine of up to N500, 000 or both.[69]

By *section 47*, all relevant law enforcement agencies are generally vested with the powers to prosecute offenders under

---

[67] Such as a levy of 0.005 on all electronic transactions by the businesses listed in the second schedule, viz. : GSM service providers and all telecommunication companies; internet service providers; banks and other financial institutions; insurance companies and the Nigerian Stock Exchange. This levy is by section 44(4) required to be remitted directly by the affected business or organization into the Fund within a period of 30 days.

[68] Section 45(1)

[69] Section 46

the Act without prejudice to the overreaching powers of the AGF.[70] However, for the offences created under *sections 19 and 21,* prosecution must be with the prior approval of the AGF. Under *Section 48,* the court may order a convicted person to forfeit to the Nigerian government, assets, money, property related to the offence. Where such assets or properties are in a foreign country, their forfeiture is subject to any treaty or arrangement with the foreign country. Additionally, under *section 49*, the court shall order for payment of compensation or restitution to victims enforceable by either the victim or the prosecutor on behalf of the victim.

2.7 PART VII- JURISDICTION AND INTERNATIONAL COOPERATION

By *section 50 (1),* the court vested with jurisdiction to try offences under the Act is the Federal High Court (FHC) located anywhere in Nigeria regardless of the location where the offence is committed.[71] For the FHC to be seized with jurisdiction however, the offence must have been committed:

a) in Nigeria; or
b) in a ship or aircraft registered in Nigeria; or
c) by a citizen or resident of Nigeria, if the person's conduct would also constitute an offence under the law of the country where the offence was committed; or
d) outside Nigeria, where–
    (i) the victim of the offence is a citizen or resident of Nigeria; or
    (ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution.

There are some Conflict of Law issues with respect to the provision where the offence is not committed in Nigeria. Generally speaking, Nigerian law would not have applicability outside the boundaries of Nigeria and it goes against the basic principles of criminal law to criminalize extra-territorial acts.

---

[70] Section 174 of the 1999 Constitution of the Federal Republic of Nigeria (as amended)

[71] In essence, Judicial Divisions do not matter. An offence committed in Ibadan, Oyo State is triable by the FHC, Taraba Division, Jalingo.

But Cybercrime is by nature, transnational hence the added jurisdictional provisions.
The proof of the facts identified in *section 50(2)* is corroborative evidence which the court is permitted to consider.[72]

By *section 50 (4)*, applications for stay of proceedings are not entertained until judgment. The mischief to be cured by this provision is unnecessary delays. *Section 306* of the Administration of Criminal Justice Act, 2015 (ACJA) has a similar provision to *section 50(4)*.

The framers of the Act in apparent realization of the transnational nature of cybercrimes provide under *section 51* that offences under the Act are extraditable under the *Extradition Act*.[73] Extradition, no doubt, reinforces the global amity against cyber criminality and ensures there is no hiding place for cybercriminals anywhere in the world. In furtherance of the need for concerted international efforts to combat the scourge of cybercrime, the AGF may request for and receive assistance from any agency or authority of a foreign state to investigate or prosecute offences under the Act. As well, he may authorize or participate in any joint investigation or prosecution for the purpose of detecting, preventing, responding to or prosecuting any offence under the Act.[74]
Section 53 makes admissible in Nigerian courts, evidence gathered in a foreign country if same is authenticated by a judge, magistrate, notary public or by sworn oath or affirmation of a witness or sealed with official or public seal of the ministry or department of the foreign state.[75]*Section 54* makes ample provisions for the form of a request to a foreign state pursuant to the Act. Nigeria may be requested to expedite the preservation of electronic device or data stored in a computer system, or network, referring to crimes described under the Act or any other enactment, pursuant to the submission of a request

[72] Such as that an accused person possesses pecuniary resources or property which he cannot satisfactorily account for or which is disproportionate to his known income.
[73] CAP E25 LFN 2004
[74] Section 52
[75]Cf admissibility of foreign evidence under section 106(h) of Evidence Act

for assistance for search, seizure and disclosure of those data.[76] In executing the request, the AGF may order any person who has the control or availability of such data, including a service provider, to preserve them or turn them in for proper preservation by an appropriate authority or person.[77] Any Nigerian law enforcement agency, may apply (ex parte if there is urgency or danger in delay) for an order of court for preservation of data, notwithstanding the provisions of *section 55(3).*[78] Under *section 56,* the ONSA is required to establish and maintain a contact point to provide immediate assistance for international cooperation. The contact point is required to be available "twenty four hours a day and seven days a week".

2.8 PART VIII- MISCELLANEOUS

The power to make delegated legislation subsidiary to the Act is vested in the AGF. The delegated legislation hereunder may be in the form of "orders, rules, guidelines or regulations as are necessary for the efficient implementation of the provisions of this Act."[79] Under *section 57(2),* the subsidiary legislation would provide for:

(a) method of custody of video and other electronic recordings of suspects apprehended under the Act;
(b) method of compliance with regulations or conventions issued by relevant international institutions on cyber security and cybercrimes;
(c) procedure for freezing, unfreezing and providing access to frozen funds or other assets;
(d) procedure for attachments, forfeiture and disposal of assets,
(e) mutual legal assistance,
(f) procedure for the prosecution of all cybercrime cases in line with national and international human rights standards;

[76] Section 55 (1)
[77] Section 55 (3)
[78] Section 55 (4)
[79] Section 57 (1)

(g) procedure for ensuring prompt payment of any levy prescribed under the Act, including penalties and prosecution; and
(h) any other matter the Attorney General may consider necessary or expedient for the purpose of the implementation of the Act.

Section 58 provides a list of definition for some terms used in the Act. It is the interpretation section. *Section 59* is the citation section.

3. HOW DOES THE ACT STACK UP AMONGST OTHER GLOBAL ANTI-CYBERCRIME INITIATIVES?

3.1 UNITED NATIONS: THE UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC) CYBERCRIME STUDY 2013 (THE STUDY)

A key finding of the Study is that legislation is pivotal in preventing and combating cybercrime. Legal measures are required in all areas, including criminalisation, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. A perusal of the Act shows that it keeps faith with this key finding. On criminalisation, the Study found that 14 acts are commonly criminalised in cybercrime legislations.[80] The Act criminalises these acts. The Study also found that several countries have adopted cyber-specific crimes for computer-related fraud, forgery and identity offences. This is true of the Act. Another finding of the Study is that International Human Rights Law

[80] Illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal data interference or system interference; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright and trademark offences; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution or possession of child pornography; computer-related solicitation or 'grooming' of children; and computer-related acts in support of terrorism offences.

acts both as a sword and a shield, requiring criminalisation of (limited) extreme forms of expression, while protecting other forms. Criminalised forms of expression include defamation, contempt, threats, incitement to hatred, insult, and obscene material, incitement to genocide and incitement to terrorism. The Act also keeps faith here.

On law enforcement and investigations, the Study finds that authorities generally use search and seizure for the physical appropriation of computer equipment and the capture of computer data. The Act provides for the powers of search and seizure. The relationship between law enforcement and internet service providers in the investigation and enforcement process is an intricate one. Whereas some countries use court orders to obtain evidence from service providers, in other countries, law enforcement may be able to obtain the necessary evidence directly. The Act accommodates both methods. The Study finds that there is a need to balance privacy and due process, with disclosure of evidence in a timely manner, in order to ensure that the private sector does not become a 'choke-point' for investigations. This is well reflected in the Act.

Cybercrime is a transnational crime and in that context, anti-cybercrime initiatives address issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence and international cooperation. The Act addresses these issues. Where they arise, jurisdictional conflicts are usually resolved through formal and informal consultations between countries. Forms of international cooperation include extradition, mutual legal assistance, and mutual recognition of foreign judgments amongst others. Due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data.

3.2 THE COUNCIL OF EUROPE: CONVENTION ON CYBERCRIME MADE AT BUDAPEST, 2001 (THE BUDAPEST CONVENTION)

The preamble of the Convention recites, inter alia, that state parties were:

> -convinced of the critical need to pursue a common anti-cybercrime policy, *inter alia,* by adopting appropriate legislation and fostering international co-operation;
> -conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;
> - concerned about the potential negative use of computer networks and electronic information;
> -mindful of the need to ensure a proper balance between the interest of law enforcement and respect for fundamental human rights.

Chapter II of the Convention identifies the "measures to be taken at the national level" against cyber-crime. *Section 1* thereof is on the measures with respect to "substantive criminal law." and provides for among others, "computer related forgery", "computer related fraud", "offences related to child pornography", "offences related to infringements of copyright and related rights", "attempt, aiding or abetting" and "corporate liability". The Convention mandates State Parties to punish natural persons who transgress the criminal provisions by effective, proportionate and dissuasive sanctions. Legal persons who transgress the criminal law provisions are to be meted similar criminal or non-criminal sanctions, including monetary sanctions. *Section 2* of Chapter 2 is with respect to "Procedural Law" such as "expedited preservation of stored computer data", "production order" and "search and seizure of stored computer data". *Section 3* of Chapter 2 is on "Jurisdiction" and provides that a state party should adopt legislative and other measures to establish jurisdiction over the offences established in accordance with the Convention.

Chapter III of the Convention makes provisions on "International cooperation" such as "principles relating to extradition"; and "General principles relating to mutual assistance" *Article 35* mandates state parties to designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings

concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. *Article 36* provides that the Convention is open for signature by the member States of the Council of Europe and by the non-member States who have participated in its elaboration. *Article 37* provides that after the entry into force of the Convention, the Committee of Ministers of the Council of Europe may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to the Convention.

The Budapest Convention is the first real international effort at cyber security. It has an established status for its model provisions. Nigeria is certainly not a member of the Council of Europe; it did not participate in the elaboration of the Convention and has yet to accede to the Convention. In Africa, South Africa has acceded to the Convention. Despite not acceding to the Convention, it is apparent that the Act is substantially in tandem with the Convention in many areas such as the provisions on substantive criminal law, on procedural law, on jurisdiction, on powers of search and arrest, on penalties and sanctions for both natural and legal persons and on international cooperation.

3.3 AFRICAN UNION: AU CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION MADE AT MALABO, 27TH JUNE 2014

As per its preamble, the AU Convention embodies existing commitments of AU member states to build the information society. It reaffirms and takes into consideration the need to respect human rights as it aims to harmonize cyber legislation in Africa. *Chapter 1* of the Convention is entitled "Electronic Transactions" and contains provisions on e-commerce. *Chapter 2* of the Convention makes provisions on Personal Data Protection. Regrettably, the profound provisions of Chapters 1 and 2 of the AU Convention are not replicated in the Act. Probably, this is because the provisions are not directly on cybercrime.

Chapter 3 is where the Act meets with the Convention. *Section I* thereof obliges member states to adopt cyber security

measures. In *Article 24*, member states are to adopt a National Policy and a National Strategy on cyber security. Nigeria has done so. By *Article 25*, member states are to adopt legal measures on cybercrime to include legislation against cybercrimes; national regulatory authorities; rights of citizens; protection of critical infrastructure. The Act confers roles for law enforcement agents, makes provisions to protect the rights of citizens as well as to protect critical infrastructure. *Article 28* is on international cooperation: harmonization; mutual legal assistance; exchange of information; means of cooperation. These issues are reflected in the Act.

Section II of Chapter 3 is on the criminal provisions to be reflected in member states anti cyber-crime legislations. The Convention directs member states to criminalise attacks on computer systems; computerized data breaches; content related offences (child pornography, pornography, racism, xenophobia, threats, insults, genocide, etc) and offences relating to electronic message security measures. *Article 30* aims to adapt certain offences to ICT- property offences such as theft, fraud, extortion, abuse of trust, blackmail, terrorism and money laundering. On criminal liability, the Convention directs member states to provide criminal sanctions that are effective, proportionate and dissuasive for both natural persons and legal persons. These provisions are well reflected in the Act.

3.4 ECONOMIC COMMUNITY OF WEST AFRICAN STATES: DIRECTIVE C/DIR. 1/08/11 ON FIGHTING CYBERCRIME WITHIN ECOWAS MADE AT ABUJA, 2011 (THE DIRECTIVE)

The Preamble to the Directive recognizes that the use of the internet has generated an "upsurge of reprehensible acts." It then notes that cyber crime is a new phenomenon requiring the definition of specific offences that must be substantially linked with conventional offences. The Directive, therefore, aims at the adoption of a framework for criminal liability in order to effectively fight cybercrime in the sub-region. The objective, according to *Article 2*, is to adapt the substantive criminal law and criminal procedure of ECOWAS member states to address the cybercrime phenomenon.

Chapter 2 of the Directive contains the substantive cybercrime offences: fraudulent access to computer systems, fraudulent remaining in a computer system, interfering with the operation of a computer system; fraudulent input of data in a computer system; fraudulent interception of computer data; fraudulent modification of computer data; computer data forgery; obtaining benefit from computer related fraud; fraudulent manipulation of computer data; use of forged data; obtaining equipment to commit an offence; child pornography; racism and xenophobia and; threat through computer system. These offences are reflected in the Act. The Directive also provides for liability of corporate bodies, search and access to computer systems by enforcement agents, expedited preservation of data as well as cooperation between member states. All these are reflected in the Act.

4. CONCLUSION

4.1 KEY POINTS OF THE ACT

We are of the opinion that the following constitute the key points of the Act:

a. It is the first Nigerian law primarily enacted to criminalise the negative use of cyberspace. It fills the void of cybercrime legislation that has long eluded the Nigerian legal system and gives the requisite peace of mind to all who work, transact or play on the internet. A host of unscrupulous cyber conducts such as spamming, phishing, cyber-squatting, cyber-stalking, cyber-fraud, identity theft, cyber-terrorism, racism and xenophobia as well as child pornography have been criminalised and ascribed punishments. In our opinion, the punishment for cyber-fraud in *section 14(2)* is stiff enough, and should, hopefully deter the so-called "yahoo-yahoo" boys. The provision of *section 15* on theft of e-devices such as ATMs is commended for being futuristic enough to include financial institutions infrastructure terminals like POS devices.
b. The Act does not create a new agency for its administration. Also, it does not leave its enforcement

to any single law enforcement agency- all law enforcement agencies can enforce the provisions of the Act. The ONSA superintends the administration of the Act while the AGF coordinates enforcement. Policy issues are to be decided by the Council.

c. The Act grants the law enforcement agents the powers of arrest, seizure, search, interception and prosecution.
d. The Act punishes attempts, aiding and abetting, counseling, procurement and conspiracy same as principal offence.
e. The Act provides for making good in monetary terms, the value of loss incurred as well as for forfeiture, restitution and compensation.
f. The Act provides for the designation of certain infrastructure as constituting CNII. However, it has been argued[81] that this provision -whose inclusion was advocated by several telecommunications stakeholders because of the spate of attacks on their infrastructure - could be a poisoned chalice. This is because by *section 3(2)*, the Presidential Order designating CNIIs may prescribe guidelines, minimum standards or rules in respect of "access to, transfer and control of data in any CNII" as well as "storage or archiving of data or information regarded as CNII". Under the Nigerian Communications Act and guidelines thereto, where a law enforcement or security agency wants to access records of a telecommunication company and the company resists, the agency must obtain court order to do so. But this provision is, effectively, a short cut for the agency.
g. The Act mandates cybercafés to register with the CPN. We fail to find a satisfactory justification for this and argue that this does not support the "ease of doing business" policy. We however, commend the introduction of a sign-in register to monitor users of cybercafés.

[81]Lambo J., & Oghenochukwu G., 2014. Cybersecurity Bill 2013- ray of hope or poisoned chalice? *op.cit*

h. The Act provides for the lawful interception of data and electronic communication. This provision would instigate issues relating to the constitutionally guaranteed right of citizens to their privacy.
i. The Act creates duties for financial institutions and for service providers. Some argue that the regulation of financial institutions is needless.[82] We see no harm in the provisions.
j. The Act validates electronic signature for transactions. This is commendable.
k. (k.) The Act invests the AGF with mandate to issue regulations and orders relating to cyber crime. This provision is crucial because it presents an opportunity for clarification and specification of grey areas in the Act as well as for attuning the Act to meet future needs.
l. (l.) The Act creates the Fund. However, while it specified sources of funds into the Fund, record keeping and auditing of the Fund, it failed to specify the utilization of the Fund apart from that up to 40% may be used for counter violent extremism programs. It is also contended that the impact of the Fund is doubtful and the levy of 0.005 of all electronic transactions may not deliver since "with a trillion or so worth of transactions, someone put the number that is likely to result to the fund at N600m"[83]
m. (m.) The FHC has exclusive jurisdiction to try offences under the Act. Though this may be good for specialization, the FHC could end up been overburdened.

4.2 RECOMMENDATIONS

From all that has been said, there are areas of challenges with the Act. Below are some of these areas for which we proffer

[82]Onyekwere, J., 2015. Cybercrimes Act 2015 and need for further amendments; *The Guardian Nigeria*, http:www.guardian.ng/features/cybercrimes-act-20150-and-need-for-further-amendments/
[83] Ibid.

recommendations in the implementation of the Act and for its future review.

a.) In line with Chapters 2 and 3 of the AU Convention as discussed above, we believe that a review of the Act to accommodate electronic commerce (in view of the prevalence of electronic transactions in the country today) as well as personal data protection would be apt. Quite apart from criminalization, a review of the Act should make far reaching provisions for overall Cybersecurity. Indeed, the Act may be renamed Cyber-security Act to provide for all matter related to the security of the internet and not just crimes.

b.) The ONSA who is conceived as the chief administrator of the Act should be up and doing. So far, there is a poor administration of the Act. For example, little or nothing is known of the ngCERT, the Fund and the 24/7 contact point. Also, the ONSA is yet to prod the President on the designation of CNIIs.

c.) The AGF is not doing a better job either. The AGF is conceived as chief enforcer of the law. He should ensure that the law enforcement agencies are capacitated to enforce the Act. The country is also, still awaiting the subsidiary rules to the Act by the AGF. Such rules could go a long way to provide need structure and vigour to the Act.

d.) Section 50(3) provides that all matters brought to the court by the "Commission" shall be conducted with dispatch and given accelerated hearing. Which commission? There is nowhere in the Act where a "Commission" is referred to and *section 58* has no such definition. This provision is obtuse. There is no reason to give preferential treatment to any Commission over all the other law enforcement agencies who are vested with prosecutorial powers under the Act. A better drafting is to provide a general provisions encouraging expedited disposal of all offences prosecuted under the Act.

e.) Section 7 provides that cybercafés should do a "business name registration" with the CAC. This provision should have simply read "business

registration". This is because a cybercafé owner is, under the provisions of the Companies and Allied Matters Act,[84] at much liberty to register his business as an incorporated entity under Part A as well as a business name under Part B. With the drive towards "ease of doing business", the other requirement for cybercafés to register with the CPN may be seen as cumbersome.

f.) Under Section 19, where a security breach occurs, the proof of negligence lies on the customer to prove that the financial institution in question could have done more to safeguard the integrity of its information. This provision turns logic on its head. The customer does not know the internal protocols of the financial institution. It is rational that in a situation like this, the *res ipsa loquitor* doctrine should apply and, the financial institution should be mandated to rebut the presumption by positive proof that they have done enough to safeguard the information. In company law, the case of *Royal British Bank vs Turquand*[85] established "*the rule in Turquands case*" or "*the indoor management principle"* which is to the effect that people transacting business with a company are entitled to assume that internal company rules are complied with, even if they are not. A variant of this rule should have applied here.

g.) We see no difference between the offence created by section 16(3) and the one created by section 8? It appears that the inclusion of a section 16(3) in the Act is inelegance in legislative drafting. The offences created in the two sections are conterminous - the penalties are same and the elements are same. The only difference perhaps is the addition of "for fraudulent purposes" in section 8. At that rate, the provision in section 8 is not only broader but completely subsumes the provision of section 16(3). There, is therefore, in our considered view, no need for section 16 (3).

h.) Section 23 (2) should be drafted more elegantly to provide that the word "other" relates to pornography

[84] CAP C20, LFN 2004
[85] (1856) 6 E&B 327

other than child pornography. Also, the subsection talks of "pornographic images" not "pornographic materials". "Pornographic materials" is more encompassing. Pornographic materials in format of videos and voice as distinct from images would seem not to have been captured by subsection 2. Therefore "materials" should replace "images".

4.3 Concluding Remarks

Despite all and as discussed in section 3 of this article, the Act, for the most part meets up with the international, regional and sub-regional anti-cybercrime initiatives. In the words of Mr. Basil Udotai, the pioneer Director and Head of the Directorate for Cybersecurity at the ONSA:

> *"The Cybercrime Act though long in coming and beset with certain challenging components, may be applied to effectively tackle Nigeria's cybercrime and cybersecurity challenges. But deliberate efforts have to be made by the key players; the ONSA and OAGF working with stake-holders to make this a reality."*[86]

Therefore, notwithstanding the real and perceived shortcomings or challenges of the Act,[87] all it takes for the Act to make the difference is concerted efforts and unity of purpose. If the ONSA and AGF provide the needed drive and superintendence, the law enforcement agents are capacitated to effectively enforce the Act, the Federal High Court is capacitated to effectively adjudicate on matters relating to the Act, and other stakeholders such as the financial institutions, internet service providers and telecommunication companies do their bit, then there would be a realisation of the purpose of the Act.

---

[86] Ibid.

[87] Ogunseide, T. (2015) Analysis: Nigeria Cybercrimes Act 2015: What are the issues? *Technology Times* Retrieved 4th May, 2018 http://technologytimes.ng/analysis-nigeria-cybercrimes-act-2015-issues/